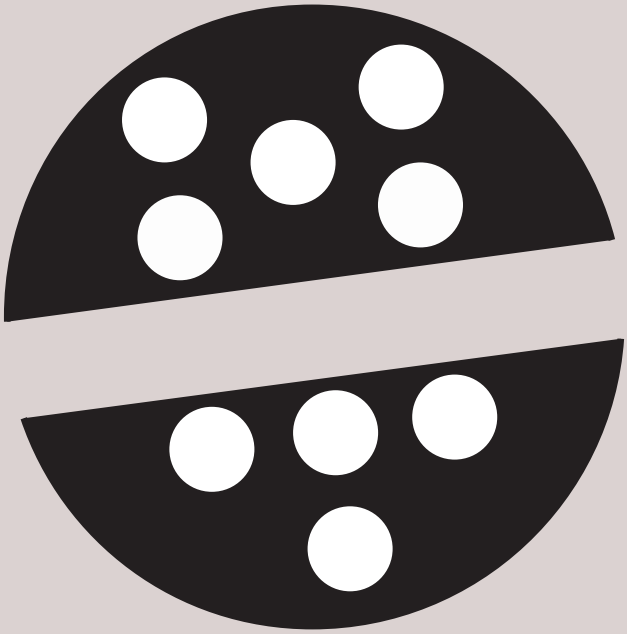
Number 14 Year 2016

Journal of New Theory

ISSN: 2149-1402



Editor-in-Chief
Naim Çağman

www.dergipark.org.tr/en/pub/jnt

Journal of New Theory (abbreviated by J. New Theory or JNT) is a mathematical journal focusing on new mathematical theories or the applications of a mathematical theory to science.

JNT founded on 18 November 2014 and its first issue published on 27 January 2015.

ISSN: 2149-1402

Editor-in-Chief: Naim Çağman

Email: journalofnewtheory@gmail.com

Language: English only.

Article Processing Charges: It has no processing charges.

Publication Frequency: Quarterly

Publication Ethics: The governance structure of J. New Theory and its acceptance procedures are transparent and designed to ensure the highest quality of published material. Journal of New Theory adheres to the international standards developed by the Committee on Publication Ethics (COPE).

Aim: The aim of the Journal of New Theory is to share new ideas in pure or applied mathematics with the world of science.

Scope: Journal of New Theory is an international, online, open access, and peer-reviewed journal. Journal of New Theory publishes original research articles, reports, reviews, editorial, letters to the editor, technical notes etc. from all branches of science that use the theories of mathematics.

Journal of New Theory concerns the studies in the areas of, but not limited to:

· Fuzzy Sets,

· Soft Sets,

· Neutrosophic Sets,

· Decision-Making

· Algebra

· Number Theory

· Analysis

· Theory of Functions

· Geometry

· Applied Mathematics

· Topology

· Fundamental of Mathematics

· Mathematical Logic

· Mathematical Physics

You can submit your manuscript in any style or JNT style as pdf. However, you should send your paper in JNT style if it would be accepted. The manuscript preparation rules, article template (LaTeX) and article template (Microsoft Word) can be accessed from the following links.

- Manuscript Preparation Rules
- Article Template (Microsoft Word.DOC) (Version 2019)
- Article Template (LaTeX) (Version 2019)

Pabitra Kumar Maji

Department of Mathematics, Bidhan Chandra College, Asansol 713301, Burdwan (W), West Bengal, India.
email: pabitra_maji@yahoo.com

Harish Garg

School of Mathematics, Thapar Institute of Engineering & Technology, Deemed University, Patiala-147004, Punjab, India
email: harish.garg@thapar.edu

Jianming Zhan

Department of Mathematics, Hubei University for Nationalities, Hubei Province, 445000, P. R. C.
email: zhanjianming@hotmail.com

Surapati Pramanik

Department of Mathematics, Nandalal Ghosh B.T. College, Narayanpur, Dist- North 24 Parganas, West Bengal 743126, India
email: sura_pati@yaho.co.in

Muhammad Irfan Ali

Department of Mathematics, COMSATS Institute of Information Technology Attock, Attock 43600, Pakistan
email: mirfanali13@yahoo.com

Said Broumi

Department of Mathematics, Hassan II Mohammedia-Casablanca University, Kasablanka 20000, Morocco
email: broumisaid78@gmail.com

Mumtaz Ali

University of Southern Queensland, Darling Heights QLD 4350, Australia
email: Mumtaz.Ali@usq.edu.au

Oktay Muhtaroğlu

Department of Mathematics, Tokat Gaziosmanpaşa University, 60250 Tokat, Turkey
email: oktay.muhtaroglu@gop.edu.tr

Ahmed A. Ramadan

Mathematics Department, Faculty of Science, Beni-Suef University, Beni-Suef, Egypt
email: aramadan58@gmail.com

Sunil Jacob John

Department of Mathematics, National Institute of Technology Calicut, Calicut 673 601 Kerala, India
email: sunil@nitc.ac.in

Aslıhan Sezgin

Department of Statistics, Amasya University, Amasya, Turkey
email: aslihan.sezgin@amasya.edu.tr

Alaa Mohamed Abd El-latif

Department of Mathematics, Faculty of Arts and Science, Northern Border University, Rafha, Saudi Arabia
email: alaa_8560@yahoo.com

Kalyan Mondal

Department of Mathematics, Jadavpur University, Kolkata, West Bengal 700032, India
email: kalyanmathematic@gmail.com

Jun Ye

Department of Electrical and Information Engineering, Shaoxing University, Shaoxing, Zhejiang, P.R. China
email: yehjun@aliyun.com

Ayman Shehata

Department of Mathematics, Faculty of Science, Assiut University, 71516-Assiut, Egypt
email: drshehata2009@gmail.com

İdris Zorlutuna

Department of Mathematics, Cumhuriyet University, Sivas, Turkey
email: izorlu@cumhuriyet.edu.tr

Murat Sarı

Department of Mathematics, Yıldız Technical University, İstanbul, Turkey
email: sarim@yildiz.edu.tr

Daud Mohamad

Faculty of Computer and Mathematical Sciences, University Teknologi Mara, 40450 Shah Alam, Malaysia
email: daud@tmsk.uitm.edu.my

Tanmay Biswas

Research Scientist, Rajbari, Rabindrapalli, R. N. Tagore Road, P.O.- Krishnagar Dist-Nadia, PIN-741101, West Bengal, India
email: tanmaybiswas_math@rediffmail.com

Kadriye Aydemir

Department of Mathematics, Amasya University, Amasya, Turkey
email: kadriye.aydemir@amasya.edu.tr

Ali Boussayoud

LMAM Laboratory and Department of Mathematics, Mohamed Seddik Ben Yahia University, Jijel, Algeria
email: alboussayoud@gmail.com

Muhammad Riaz

Department of Mathematics, Punjab University, Quaid-e-Azam Campus, Lahore-54590, Pakistan
email: mriaz.math@pu.edu.pk

Serkan Demiriz

Department of Mathematics, Tokat Gaziosmanpaşa University, Tokat, Turkey
email: serkan.demiriz@gop.edu.tr

Hayati Olğar

Department of Mathematics, Tokat Gaziosmanpaşa University, Tokat, Turkey
email: hayati.olgar@gop.edu.tr

Essam Hamed Hamouda

Department of Basic Sciences, Faculty of Industrial Education, Beni-Suef University, Beni-Suef, Egypt
email: ehamouda70@gmail.com

Layout Editors

Tuğçe Aydın

Department of Mathematics, Çanakkale Onsekiz Mart University, Çanakkale, Turkey
email: aydinttugce@gmail.com

Fatih Karamaz

Department of Mathematics, Çankırı Karatekin University, Çankırı, Turkey
email: karamaz@karamaz.com

Contact

Editor-in-Chief
Name: Prof. Dr. Naim Çağman
Email: journalofnewtheory@gmail.com
Phone: +905354092136
Address: Departments of Mathematics, Faculty of Arts and Sciences, Tokat Gaziosmanpaşa University, Tokat, Turkey

Editors
Name: Assoc. Prof. Dr. Faruk Karaaslan
Email: karaaslan.faruk@gmail.com
Phone: +905058314380
Address: Departments of Mathematics, Faculty of Arts and Sciences, Çankırı Karatekin University, 18200, Çankırı, Turkey

Name: Assoc. Prof. Dr. İrfan Deli
Email: irfandeli@kilis.edu.tr
Phone: +905426732708
Address: M.R. Faculty of Education, Kilis 7 Aralık University, Kilis, Turkey

Name: Asst. Prof. Dr. Serdar Enginoğlu
Email: serdarenginoglu@gmail.com
Phone: +905052241254
Address: Departments of Mathematics, Faculty of Arts and Sciences, Çanakkale Onsekiz Mart University, 17100, Çanakkale, Turkey

CONTENT

http://www.newtheory.org **ISSN: 2149-1402**

Journal of New Theory

Received: 21.02.2016 *Year*: **2016**, *Number*: **14**, *Pages*: **01-09**
Published: 20.06.2016 *Original Article*[**]

ON STEREOGRAPHIC CIRCULAR WEIBULL DISTRIBUTION

Phani Yedlapalli[1,*] <phaniyedlapalli23@gmail.com>
Sagi Venkata Sesha Girija[2] <svs.girija@gmail.com>
Akkavajhula Venkata Dattatreya Rao[3] <avdrao@gmail.com>

[1]*Department of Basic Science, Shri Vishnu Engineering College for Women, Vishnupur, Bhimavaram-534221, Andhra Pradesh, India.*
[2]*Department of Mathematics, Hindu College, Guntur, Andhra Pradesh, India*
[3]*Department of Statistics, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India.*

Abstract – In this paper, we introduce Stereographic-l-axial Weibull and Stereographic Circular Weibull distributions for modeling l-axial and circular data by extending the Stereographic Semicircular Weibull distribution [8]. Discussed the estimation of parameters also and derived the first two trigonometric moments for the proposed Stereographic Circular Weibull model.

Keywords *– Semicircular models, l-axial data, Stereographic projection, Trigonometric moments.*

1 Introduction

In some of the cases the directional / angular data does not required full circular models for modeling, this fact is noted in Guardiola [3], Jones [5], Byoung et al [1] and Yedlapalli et at [8]. For example, when sea turtles emerge from the ocean in search of a nesting site on dry land, a random variable having values on a semicircle is well sufficient for modeling such data. Similarly, when an aircraft is lost but its departure and its initial headings are known, a semicircular random variable is sufficient for such angular data. And few more examples of semicircular data is available in Ugai et al [10].

Toshihiro Abe et al [11] constructed some Unimodal and symmetric distributions by applying Inverse Stereographic projection, Yedlapalli et al [8] constructed some semicircular distributions by applying Inverse Stereographic projection. In this paper we developed the Stereographic- l-axial Weibull distribution by extending the Stereographic Semicircular Weibull and observed that Stereographic Circular Weibull distribution is a

[**]*Edited by* Oktay Muhtaroğlu *(Area Editor) and* Naim Çağman *(Editor-in-Chief).*
[*]*Corresponding Author.*

special case to proposed model and also Stereographic Circular Exponential [9] and Stereographic Circular Rayleigh Distributions are special cases to Stereographic Circular Weibull Distribution, where the same is true in linear case also . We plotted the graphs of the density function for various values of parameters. First two trigonometric moments for proposed model are derived, we estimate parameters of the Stereographic Circular Weibull model by a maximum likelihood method.

2 Stereographic-l-axial Weibull Distribution

Here we recall the definition of Stereographic Semicircular Weibull Distribution [8].

Definition 2.1 (Stereographic Semicircular Weibull Distribution) A random variable θ on unit semicircle is said to have Stereographic Semicircular Weibull distribution with shape parameter $c>0$ and scale parameter $\sigma>0$ denoted by $\mathrm{SCW}(c,\sigma)$, if the probability density and cumulative distribution functions are given by

1. $$g(\theta)=\frac{c}{2\sigma}\sec^2\left(\frac{\theta}{2}\right)\left(\tan\left(\frac{\theta}{2}\right)\right)^{c-1}\exp\left(\frac{1}{\sigma}\left(\tan\left(\frac{\theta}{2}\right)\right)^{c}\right),\ \text{for}\ 0\le\theta<\pi, c>0\ \text{and}\ \sigma>0$$

2. $$G(\theta)=1-e^{-\frac{1}{\sigma}\left(\tan\left(\frac{\theta}{2}\right)\right)^{c}}$$

We extend the above Stereographic Semicircular Weibull model [8] to the l -axial distribution, which is applicable to any arc of arbitrary length say $2\pi/l$ for $l=1,2,...,$ so it is desirable to extend the Stereographic Semicircular Weibull distribution[8] to construct the Stereographic-l-axial Weibull distribution, we consider the density function of Stereographic Semicircular Weibull distribution and use the transformation $\phi=2\theta/l$, $l=1,2,...,$. The probability density function of ϕ is given by

$$g(\theta)=\frac{cl}{4\sigma}\sec^2\left(\frac{l\theta}{4}\right)\left(\tan\left(\frac{l\theta}{4}\right)\right)^{c-1}\exp\left(-\frac{1}{\sigma}\left(\tan\left(\frac{l\theta}{4}\right)\right)^{c}\right),$$

$$0<\theta<\frac{2\pi}{l},\ \sigma>0,\ c>0\ \text{and}\ l=1,2,.. \qquad (2.1.1)$$

We call it as **Stereographic -l-axial Weibull distribution**

Case (1) When $l=1$, in the probability density function (2.1.1), we get the density function

$$g(\theta)=\frac{c}{4\sigma}\sec^2\left(\frac{\theta}{4}\right)\left(\tan\left(\frac{\theta}{4}\right)\right)^{c-1}\exp\left(-\frac{1}{\sigma}\left(\tan\left(\frac{\theta}{4}\right)\right)^{c}\right),$$

$$0<\theta<2\pi,\ \sigma>0 \text{ and } c>0 \tag{2.1.2}$$

We call it as **Stereographic Circular Weibull distribution**.

Case (2) When $l=2$, the probability density function (2.1.1) is the same as that of **Stereographic Semicircular Weibull Distribution** [8].

2.2 Stereographic Circular Weibull Distribution

A random variable X_S on a unit circle is said to have Stereographic Circular Weibull Distribution with scale parameters $\sigma>0$, shape parameter $c>0$ and location parameter μ denoted by **SCWD**(c,σ,μ). If its probability density and cumulative distribution functions are given by

$$g(\theta)=\frac{c}{4\sigma}\sec^2\left(\frac{\theta-\mu}{4}\right)\left(\tan\left(\frac{\theta-\mu}{4}\right)\right)^{c-1}\exp\left(-\frac{1}{\sigma}\left(\tan\left(\frac{\theta-\mu}{4}\right)\right)^{c}\right),$$
$$0<\theta,\mu<2\pi,\ c>0 \text{ and } \sigma>0 \tag{2.2.1}$$

$$G(\theta)=1-e^{-\frac{1}{\sigma}\left(\tan\left(\frac{\theta-\mu}{4}\right)^{c}\right)} \tag{2.2.2}$$

Special Cases

Case1: When $c=1,$ in (2.1.1), we get the density function of **Stereographic-l- axial Exponential Distribution[9]**. i.e.,

$$g(\theta)=\frac{l}{4\sigma}\sec^2\left(\frac{l\theta}{4}\right)\exp\left(-\frac{1}{\sigma}\left(\tan\left(\frac{l\theta}{4}\right)\right)\right),\ 0<\theta<\frac{2\pi}{l},\ \sigma>0 \text{ and } l=1,2,.. \tag{2.2.3}$$

Case2: When $c=1\&l=1$, in (2.1.1), we get the density function

$$g(\theta)=\frac{1}{4\sigma}\sec^2\left(\frac{\theta}{4}\right)\exp\left(-\frac{1}{\sigma}\left(\tan\left(\frac{\theta}{4}\right)\right)\right),\ 0<\theta<2\pi,\ \sigma>0 \tag{2.2.4}$$

We call it as **Stereographic Circular Exponential Distribution [9].**

Case3: When $c=1\&l=2$, in (2.1.1), we get the density function of **Stereographic Semicircular Exponential Distribution** [8].

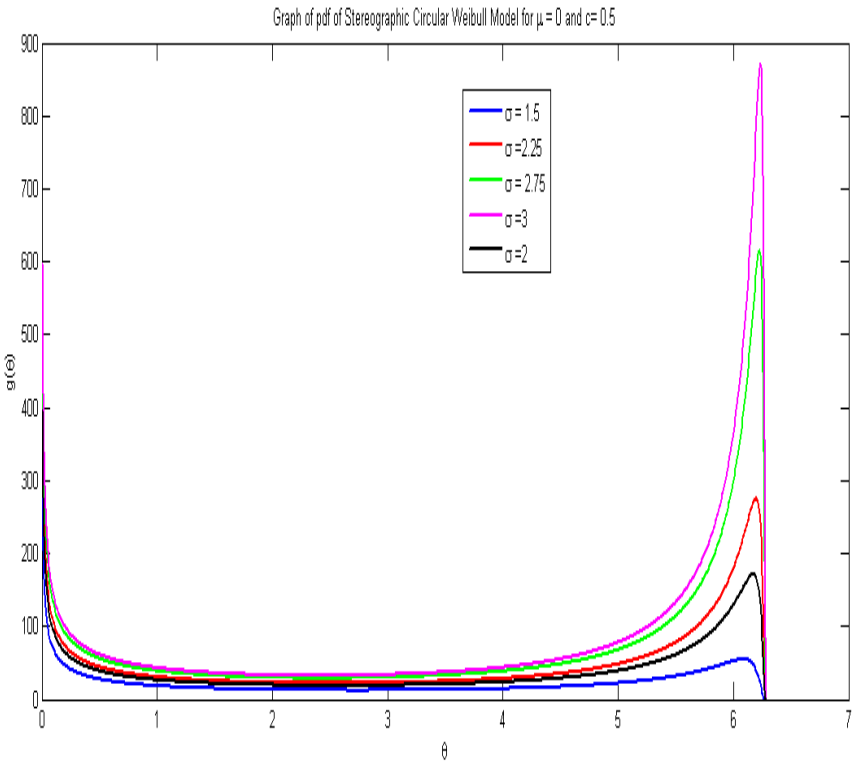
Case 4: When $c=2$ & $l=1$, in (2.1.1), we get the density function

$$g(\theta)=\frac{1}{2\sigma}\sec^2\left(\frac{\theta}{4}\right)\left(\tan\left(\frac{\theta}{4}\right)\right)\exp\left(-\frac{1}{\sigma}\left(\tan\left(\frac{\theta}{4}\right)\right)^2\right), \quad 0<\theta<2\pi,\ \sigma>0 \tag{2.2.5}$$

We call it as **Stereographic Circular Rayleigh Distribution**

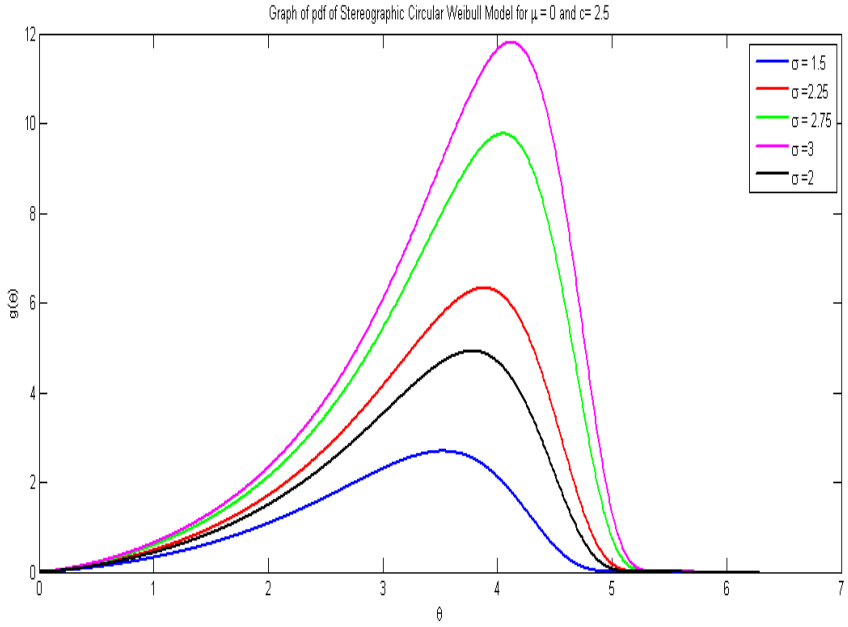
The same is true in linear case also.

2.3 Graphs of Density Function of Stereographic Circular Weibull Distribution for Various Values of the Parameters



3 Trigonometric moments of Stereographic Circular Weibull Model

Without loss of generality here we assume that $\mu=0$, in (2.1.2) .The trigonometric moments of the distribution are given by $\{\varphi_p : p=0,\pm1,\pm2,\pm3,...\}$, where $\varphi_p=\alpha_p+i\beta_p$, with $\alpha_p=E(\cos p\theta)$ and $\beta_p=E(\sin p\theta)$ being the p^{th} order cosine and sine moments of the random angle θ, respectively.



Theorem 3.1 Under the pdf of Stereographic Circular Weibull Model with $\mu=0$, the first four $\alpha_{\mathrm{p}}=E(\cos \mathrm{p}\theta)$ and $\beta_{\mathrm{p}}=E(\sin \mathrm{p}\theta)$, $\mathrm{p}=1,2.$ are given as follows:

$$\alpha_1=1-\frac{8}{\sigma}\sum_{n=0}^{\infty}(-1)^n(n+1)(\sigma)^{-\left(\frac{2n+c+2}{c}\right)}\Gamma\left(\frac{2n+c+2}{c}\right)$$

$$\beta_1=\frac{4}{\sigma}\sum_{n=0}^{\infty}(-1)^n(n+1)(\sigma)^{\left(\frac{2n+c+2}{c}\right)}\Gamma\left(\frac{2n+c+2}{c}\right)-\frac{8}{\sigma}\sum_{n=0}^{\infty}(-1)^n(n+1)(\sigma)^{\left(\frac{2n+c+4}{c}\right)}\Gamma\left(\frac{2n+c+4}{c}\right)$$

$$\alpha_2=1-\frac{32}{\sigma}\sum_{n=0}^{\infty}(-1)^n(n+1)(\sigma)^{\left(\frac{2n+c+2}{c}\right)}\Gamma\left(\frac{2n+c+2}{c}\right)$$
$$+\frac{12}{\sigma}\sum_{n=0}^{\infty}(-1)^n C(n+3,3)(\sigma)^{\left(\frac{2n+c+4}{c}\right)}\Gamma\left(\frac{2n+c+4}{c}\right)$$

$$\beta_2=\frac{8}{\sigma}\sum_{n=0}^{\infty}(-1)^n(\sigma)^{\left(\frac{2n+c+1}{c}\right)}\Gamma\left(\frac{2n+c+1}{c}\right)-\frac{16}{\sigma}\sum_{n=0}^{\infty}(-1)^n(n+1)(\sigma)^{\left(\frac{2n+c+3}{c}\right)}\Gamma\left(\frac{2n+c+3}{c}\right)$$

$$-\frac{64}{\sigma}\sum_{n=0}^{\infty}(-1)^n C(n+3,3)(\sigma)^{\left(\frac{2n+c+4}{c}\right)}\Gamma\left(\frac{2n+c+4}{c}\right)+\frac{128}{\sigma}\sum_{n=0}^{\infty}(-1)^n C(n+3,3)(\sigma)^{\left(\frac{2n+c+5}{c}\right)}\Gamma\left(\frac{2n+c+5}{c}\right)$$

Proof:

$$\varphi_{\mathrm{p}}=\int_0^{\pi}e^{ip\theta}g(\theta)d\theta=\int_0^{\pi}\cos(\mathrm{p}\theta)g(\theta)d\theta+i\int_0^{\pi}\sin(\mathrm{p}\theta)g(\theta)d\theta$$

$$= E\left(\cos\left(\mathrm{p}\theta\right)\right) + i\,E\left(\sin\left(\mathrm{p}\theta\right)\right) = \alpha_{\mathrm{p}} + i\,\beta_{\mathrm{p}} \quad \text{for } \mathrm{p} = 1, 2.$$

For the first cosine and sine moments, use the transformation $x = \tan\left(\frac{\theta}{4}\right)$,

$$\cos\theta = 1 - \frac{8x^2}{\left(1+x^2\right)^2}$$

and $\sin\theta = \frac{4x}{\left(1+x^2\right)^2} - \frac{8x^3}{\left(1+x^2\right)^2}$,the results α_1 and β_1 follows by the integral formula

3.478.1 [2]. Now

$$\mathrm{E}\left(\cos\left(\mathrm{p}\theta\right)\right) = \frac{c}{4\sigma}\int_0^{2\pi} \cos\left(\mathrm{p}\theta\right)\sec^2\left(\frac{\theta}{4}\right)\left(\tan\left(\frac{\theta}{4}\right)\right)^{c-1} e^{-\frac{1}{\sigma}\left(\tan\left(\frac{\theta}{4}\right)\right)^c} d\theta$$

and

$$\mathrm{E}\left(\sin\left(\mathrm{p}\theta\right)\right) = \frac{c}{4\sigma}\int_0^{2\pi} \sin\left(\mathrm{p}\theta\right)\sec^2\left(\frac{\theta}{4}\right)\left(\tan\left(\frac{\theta}{4}\right)\right)^{c-1} e^{-\frac{1}{\sigma}\left(\tan\left(\frac{\theta}{4}\right)\right)^c} d\theta$$

$$\alpha_1 = \frac{c}{4\sigma}\int_0^{2\pi} \cos\theta\sec^2\left(\frac{\theta}{4}\right)\left(\tan\left(\frac{\theta}{4}\right)\right)^{c-1} e^{-\frac{1}{\sigma}\left(\tan\left(\frac{\theta}{4}\right)\right)^c} d\theta$$

$$= \frac{c}{\sigma}\int_0^{\infty}\left[1 - \frac{8x^2}{\left(1+x^2\right)^2}\right] x^{c-1} e^{-\frac{1}{\sigma}x^c} dx$$

$$= 1 - \frac{8c}{\sigma}\int_0^{\infty} x^{c+1}\left(1+x^2\right)^{-2} e^{-\frac{1}{\sigma}x^c} dx$$

$$= 1 - \frac{8c}{\sigma}\int_0^{\infty} x^{c+1}\sum_{n=0}^{\infty}\left(-1\right)^n\left(n+1\right)x^{2n} e^{-\frac{1}{\sigma}x^c} dx$$

$$= 1 - \frac{8c}{\sigma}\sum_{n=0}^{\infty}\left(-1\right)^n\left(n+1\right)\frac{1}{c}\left(\frac{1}{\sigma}\right)^{-\left(\frac{2n+c+2}{c}\right)}\Gamma\left(\frac{2n+c+2}{c}\right)$$

$$\alpha_1 = 1 - \frac{8}{\sigma}\sum_{n=0}^{\infty}\left(-1\right)^n\left(n+1\right)\left(\sigma\right)^{-\left(\frac{2n+c+2}{c}\right)}\Gamma\left(\frac{2n+c+2}{c}\right)$$

$$\beta_1 = \frac{c}{4\sigma}\int_0^{2\pi} \sin\theta\sec^2\left(\frac{\theta}{4}\right)\left(\tan\left(\frac{\theta}{4}\right)\right)^{c-1} e^{-\frac{1}{\sigma}\left(\tan\left(\frac{\theta}{4}\right)\right)^c} d\theta$$

$$= \frac{c}{\sigma}\int_0^{\infty}\left[\frac{4x}{\left(1+x^2\right)^2} - \frac{8x^3}{\left(1+x^2\right)^2}\right] x^{c-1} e^{-\frac{1}{\sigma}x^c} dx$$

$$=\frac{4c}{\sigma}\int_0^{\infty}\frac{x^{c+1}}{\left(1+x^2\right)^2}e^{-\frac{1}{\sigma}x^c}dx-\frac{8c}{\sigma}\int_0^{\infty}\frac{x^{c+3}}{\left(1+x^2\right)^2}e^{-\frac{1}{\sigma}x^c}dx$$

$$=\frac{4c}{\sigma}\int_0^{\infty}x^{c+1}\sum_{n=0}^{\infty}(-1)^n(n+1)x^{2n}e^{-\frac{1}{\sigma}x^c}dx-\frac{8c}{\sigma}\int_0^{\infty}x^{c+3}\sum_{n=0}^{\infty}(-1)^n(n+1)x^{2n}e^{-\frac{1}{\sigma}x^c}dx$$

$$=\frac{4c}{\sigma}\sum_{n=0}^{\infty}(-1)^n(n+1)\int_0^{\infty}x^{(2n+c+2)-1}e^{-\frac{1}{\sigma}x^c}dx-\frac{8c}{\sigma}\sum_{n=0}^{\infty}(-1)^n(n+1)\int_0^{\infty}x^{(2n+c+4)-1}e^{-\frac{1}{\sigma}x^c}dx$$

$$\beta_1=\frac{4}{\sigma}\sum_{n=0}^{\infty}(-1)^n(n+1)(\sigma)^{\left(\frac{2n+c+2}{c}\right)}\Gamma\left(\frac{2n+c+2}{c}\right)-\frac{8}{\sigma}\sum_{n=0}^{\infty}(-1)^n(n+1)(\sigma)^{\left(\frac{2n+c+4}{c}\right)}\Gamma\left(\frac{2n+c+4}{c}\right)$$

To obtain second cosine and sine moments α_2 and β_2, we use the transformation

$$x=\tan\left(\frac{\theta}{4}\right),\quad \cos 2\theta=1+\frac{12x^4}{\left(1+x^2\right)^4}-\frac{32x^2}{\left(1+x^2\right)^2}$$

and

$$\sin 2\theta=\frac{8x}{\left(1+x^2\right)^2}-\frac{16x^3}{\left(1+x^2\right)^2}-\frac{64x^3}{\left(1+x^2\right)^4}+\frac{128x^5}{\left(1+x^2\right)^4},$$

the results of α_2 and β_2 follows by the same integral formula of α_1.

$$\alpha_2=\frac{c}{4\sigma}\int_0^{2\pi}\cos 2\theta\sec^2\left(\frac{\theta}{4}\right)\left(\tan\left(\frac{\theta}{4}\right)\right)^{c-1}e^{-\frac{1}{\sigma}\left(\tan\left(\frac{\theta}{4}\right)\right)^c}d\theta$$

$$=\frac{c}{\sigma}\int_0^{\infty}\left[1+\frac{12x^4}{\left(1+x^2\right)^4}-\frac{32x^2}{\left(1+x^2\right)^2}\right]x^{c-1}e^{-\frac{1}{\sigma}x^c}dx$$

$$=1+\frac{12c}{\sigma}\int_0^{\infty}x^{c+3}\left(1+x^2\right)^{-4}e^{-\frac{1}{\sigma}x^c}dx-\frac{32c}{\sigma}\int_0^{\infty}x^{c+1}\left(1+x^2\right)^{-2}e^{-\frac{1}{\sigma}x^c}dx$$

$$=1-\frac{32c}{\sigma}\sum_{n=0}^{\infty}(-1)^n(n+1)\int_0^{\infty}x^{(2n+c+2)-1}e^{-\frac{1}{\sigma}x^c}dx+\frac{12c}{\sigma}\sum_{n=0}^{\infty}C(n+3,3)(-1)^n\int_0^{\infty}x^{(2n+c+4)-1}e^{-\frac{1}{\sigma}x^c}dx$$

$$\alpha_2=1-\frac{32}{\sigma}\sum_{n=0}^{\infty}(-1)^n(n+1)(\sigma)^{\left(\frac{2n+c+2}{c}\right)}\Gamma\left(\frac{2n+c+2}{c}\right)$$
$$+\frac{12}{\sigma}\sum_{n=0}^{\infty}(-1)^nC(n+3,3)(\sigma)^{\left(\frac{2n+c+4}{c}\right)}\Gamma\left(\frac{2n+c+4}{c}\right),$$

$$\beta_2=\frac{c}{4\sigma}\int_0^{2\pi}\sin 2\theta\sec^2\left(\frac{\theta}{4}\right)\left(\tan\left(\frac{\theta}{4}\right)\right)^{c-1}e^{-\frac{1}{\sigma}\left(\tan\left(\frac{\theta}{4}\right)\right)^c}d\theta$$

$$=\frac{c}{\sigma}\int_0^{\infty}\left[\frac{8x}{\left(1+x^2\right)^2}-\frac{16x^3}{\left(1+x^2\right)^2}-\frac{64x^3}{\left(1+x^2\right)^4}+\frac{128x^5}{\left(1+x^2\right)^4}\right]x^{c-1}e^{-\frac{1}{\sigma}x^c}dx$$

$$=\frac{8c}{\sigma}\int_0^{\infty}x^c\left(1+x^2\right)^{-2}e^{-\frac{1}{\sigma}x^c}dx-\frac{16c}{\sigma}\int_0^{\infty}x^{c+2}\left(1+x^2\right)^{-2}e^{-\frac{1}{\sigma}x^c}dx$$

$$-\frac{64c}{\sigma}\int_0^{\infty}x^{c+3}\left(1+x^2\right)^{-4}e^{-\frac{1}{\sigma}x^c}dx+\frac{128c}{\sigma}\int_0^{\infty}x^{c+4}\left(1+x^2\right)^{-4}e^{-\frac{1}{\sigma}x^c}dx$$

$$=\frac{8c}{\sigma}\sum_{n=0}^{\infty}(-1)^n(n+1)\int_0^{\infty}x^{(2n+c+1)-1}e^{-\frac{1}{\sigma}x^c}dx-\frac{16c}{\sigma}\sum_{n=0}^{\infty}(-1)^n(n+1)\int_0^{\infty}x^{(2n+c+3)-1}e^{-\frac{1}{\sigma}x^c}dx$$

$$-\frac{64c}{\sigma}\sum_{n=0}^{\infty}(-1)^n C(n+3,3)\int_0^{\infty}x^{(2n+c+4)-1}e^{-\frac{1}{\sigma}x^c}dx+\frac{128c}{\sigma}\sum_{n=0}^{\infty}(-1)^n C(n+3,3)\int_0^{\infty}x^{(2n+c+5)-1}e^{-\frac{1}{\sigma}x^c}dx$$

$$\beta_2=\frac{8}{\sigma}\sum_{n=0}^{\infty}(-1)^n(\sigma)^{\left(\frac{2n+c+1}{c}\right)}\Gamma\left(\frac{2n+c+1}{c}\right)-\frac{16}{\sigma}\sum_{n=0}^{\infty}(-1)^n(n+1)(\sigma)^{\left(\frac{2n+c+3}{c}\right)}\Gamma\left(\frac{2n+c+3}{c}\right)$$

$$-\frac{64}{\sigma}\sum_{n=0}^{\infty}(-1)^n C(n+3,3)(\sigma)^{\left(\frac{2n+c+4}{c}\right)}\Gamma\left(\frac{2n+c+4}{c}\right)+\frac{128}{\sigma}\sum_{n=0}^{\infty}(-1)^n C(n+3,3)(\sigma)^{\left(\frac{2n+c+5}{c}\right)}\Gamma\left(\frac{2n+c+5}{c}\right)$$

In the similar process we can obtain the higher order moments also .

4 Estimation of Parameter

The minus log-likelihood for a random sample of size n, $\theta_1,\theta_2,\theta_3,...,\theta_n$, from the Circular Weibull distribution is given by

$$L(\mu,\sigma;\theta)=\prod_{i=1}^{n}g(\theta_i)=\prod_{i=1}^{n}\left[\frac{c}{4\sigma}\sec^2\left(\frac{\theta_i-\mu}{4}\right)\left(\tan\left(\frac{\theta_i-\mu}{4}\right)\right)^{c-1}\exp\left\{-\frac{1}{\sigma}\left(\tan\left(\frac{\theta_i-\mu}{4}\right)\right)^c\right\}\right] \tag{4.1}$$

$$-l\left((\mu,\sigma,c;\theta)\right)=-\log\left(L(\mu,\sigma,c;\theta)\right)=n\log(4\sigma)-n\log(c)+2\sum_{i=1}^{n}\log\left(\cos\left(\frac{(\theta_i-\mu)}{4}\right)\right)$$
$$+\left(\frac{1}{\sigma}-c+1\right)\sum_{i=1}^{n}\log\left(\tan\left(\frac{(\theta_i-\mu)}{4}\right)\right) \tag{4.2}$$

To find maximum likelihood estimates, we can use any minimization subroutine for direct minimization of the minus log-likelihood itself.

5 Conclusions

In this paper, we discussed circular distribution resulting from extending Stereographic Semicircular Weibull distribution on unit semicircle which is obtained by inducing Inverse Stereographic Projection on the real line. The density and distribution functions of

Stereographic Circular Weibull distribution admit explicit forms, as do trigonometric moments and observed that in similar to linear case, Stereographic Circular Exponential and Stereographic Circular Rayleigh distributions are Special cases to proposed Stereographic Circular Weibull Distribution. As this distribution is asymmetric, promising for modeling asymmetrical directional data.

References

[1] Byoung, J.A and Hyoung M.K.(2008). A New Family of Semicircular Models: The Semicircular Laplace Distributions, Communications of the Korean Statistical Society Vol.15, pp. 775-781.

[2] Gradshteyn and Ryzhik (2007). Table of Integrals, series and products, 7th edition, Academic Press.

[3] Guardiola, J.H. (2004). The Semicircular Normal Distribution, Ph.D Dissertation, Baylor University, Institute of Statistics.

[4] Jammalamadaka S. Rao and Sen Gupta, A. (2001). Topics in Circular Statistics, *World Scientific Press, Singapore.*

[5] Jones, T.A. (1968). Statistical Analysis of orientation data, Journal of Sedimentary Petrology, 38, 61-67.

[6] Kim, H.M.(2008). New family of the t distributions for modeling semicircular data, Communications of the Korean Statistical Society. Vol.15, N0.5, pp. 667-674.

[7] Mardia, K.V. and Jupp, P.E. (2000), Directional Statistics, *John Wiley, Chichester.*

[8] Phani Yedlapalli, Girija S.V.S., and Dattatreya Rao A.V. (2013). On Construction of Stereographic Semicircular Models, Journal of Applied Probability and Statistics. Vol 8, No. 1, pp. 75-90.

[9] Phani Yedlapalli, R.V. Babu, S.V.S.Girija and A.V.Dattatreya Rao (2015). Stereographic -l-axial Exponential and Stereographic Circular Exponential Distributions, International Journal of Scientific and Innovative Mathematical Research (IJSIMR), Vol.3, Special Issue-5 , pp. 108-114.

[10] Ugai. S.K., Nishijima, M. and Kan, T. (1977), Characteristics of raindrop size and raindrop shape, *Open symposium* URSI *Commission F,* 225-230.

[11] Toshihiro Abe, Kunio Shimizu and Arthur Pewsey, (2010), Symmetric Unimodal Models for Directional Data Motivated by Inverse Stereographic Projection, *J. Japan Statist. Soc.,* Vol. 40 (No. 1), pp. 45-61.

http://www.newtheory.org **ISSN: 2149-1402**

Journal of New Theory

Received: 13.02.2016 *Year*: **2016**, *Number*: **14**, *Pages*: **10-25**
Published: 29.06.2016 *Original Article*[**]

REFINED SOFT SETS AND ITS APPLICATIONS

Anjan Mukherjee[1,*] <anjan2002_m@yahoo.co.in>
Mithun Datta[1] <mithunagt007@gmail.com>
Abhijit Saha[2] <abhijit84_mt@yahoo.in>

[1]Department of Mathematics, Tripura University, Suryamaninagar, Agartala -799022, Tripura, INDIA
[2]Techno India, Maheshkhola, Agartala-799022, Tripura, INDIA

Abstract - Many disciplines, including engineering, economics, medical science and social science are highly dependent on the task of modeling and computing uncertain data. When the uncertainty is highly complicated and difficult to characterize, classical mathematical approaches are often insufficient to derive effective or useful models. Testifying to the importance of uncertainties that cannot be defined by classical mathematics, researchers are introducing alternative theories every day. In addition to classical probability theory, some of the most important results on this topic are fuzzy sets, intuitionistic fuzzy sets, vague sets, interval-valued fuzzy set and rough sets. But each of these theories has its inherent limitations as pointed out by Molodtsov. For example, in probability theory, we require a large number of experiments in order to check the stability of the system. To define a membership function in case of fuzzy set theory is not always an easy task. Theory of rough sets requires an equivalence relation defined on the universal set under consideration. But in many real life situations such an equivalence relation is very difficult to find due to imprecise human knowledge. Perhaps the above mentioned difficulties associated with these theories are due to their incompatibility with the parameterization tools. Molodtsov introduced soft set theory as a completely new approach for modeling vagueness and uncertainty. This so-called soft set theory is free from the above mentioned difficulties as it has enough parameters. In soft set theory, the problem of setting membership function simply doesn't arise. This makes the theory convenient and easy to apply in practice. Soft set theory has potential applications in various fields including smoothness of functions, game theory, operations research, Riemann integration, probability theory and measurement theory. Most of these applications have already been demonstrated by Molodtsov.

In this paper a new approach called refined soft sets is presented. Mathematically, this so called notion of refined soft sets may seem different from the classical soft set theory but the underlying concepts are very similar. In this paper the concept of refined soft set is introduced and the several operations between refined soft sets and soft sets are discussed. We also present the concept of soft images and soft inverse image of refined soft sets. The concept of image of a refined soft set has been used in a customer query problem.

[**] *Edited by* Irfan Deli *(Area Editor) and* Naim Çağman *(Editor-in-Chief).*
[*] *Corresponding Author.*

1. Introduction

The traditional soft set is a mapping from a parameter to the crisp subset of universe. Molodtsov [15] introduced the theory of soft sets as a generalized tool for modeling complex systems involving uncertain or not clearly defined objects. Soft set is a parameterized general mathematical tool which deals with a collection of approximate descriptions of objects. Each approximate description has two parts, a predicate and an approximate value set. In the soft set theory, the initial description of the object has an approximate nature, and we do not need to introduce the notion of exact solution. The absence of any restrictions on the approximate description in soft set theory makes this theory very convenient and easily applicable in practice. Any parameterization we prefer can be used with the help of words and sentences, real numbers, functions, mappings and so on. In recent years, soft set theory have been developed rapidly and focused by many researchers in theory and practice. Maji et al. [14] defined several operations on soft sets and made a theoretical study on the theory of soft sets. Aktas and Cagman [1] compared soft sets to the related concepts of fuzzy sets and rough sets. They also defined the notion of soft groups. Jun [10] applied soft set to the theory of BCK/BCI algebra and introduced the concept of soft BCK/BCI algebra. Jun and park [11] discussed the applications of soft sets in ideal theory of BCK/BCI algebra. Feng et al. [7] defined soft semi rings and several related notions in order to establish a connection between soft sets and semi rings. Furthermore based on [14], Ali et al. [2] introduced some new operations on soft sets and by improving the notion of complement of soft set, proved that certain De Morgan's laws hold in soft set theory. Qin and Hong [17] introduced the notion of soft equality and established lattice structures and soft quotient algebras of soft sets. Chen et al. [6] presented a new definition of soft set parameterization reduction and compared this definition to the related concept of attribute reduction in rough set theory. Kong et al. [13] introduced the notion of normal parameter reduction of soft sets and constructed a reduction algorithm based on the importance degree of parameters. Babitha and Sunil [5] made an attempt to explain the equivalent version of some theories on relations and functions in the background of soft sets. In 2011, Kharal and Ahmad [12] introduced the notion of soft images and soft inverse images and they applied these notions to the problem of medical diagnosis.

In this paper a new approach called refined soft sets is presented. Mathematically, this so called notion of ultra soft sets may seem different from the classical soft set theory but the underlying concepts are very similar. These new type of soft sets satisfy all the basic properties of soft sets. The organization of the paper is as follows: Section 2 briefly reviews some background on soft set. Section 3 focuses on the concepts and operations of refined soft sets. Moreover the basic properties of refined soft sets are presented. In section 4, we propose two different types operations between refined soft sets and soft sets. Section 5 is devoted to the discussion of soft images and soft inverse images of refined soft sets. The last section summarizes all the contributions made and points out future research work.

2. Preliminaries

In this section, some definitions and notions about soft sets are given. These will be useful in later sections.

Let U be an universe set and E be a set of possible parameters with respect to U. Usually parameters are attributes, characteristics or properties of the objects in U. Let P(U) denotes the power set of U and A,B⊆E.

Definition 2.1: [16] A pair (f, A) is called a soft set over U, where A⊆E and f is a mapping given by f: A→ P(U).

In other words, a soft set over U can be regarded as a parameterized family of subsets of U, which gives an approximation(soft) description of the objects in U. For e∈A, f(e) may be considered as the set of e-approximate elements of the soft set (f, A).

Definition 2.2: [15] For two soft sets (f,A) and (g,B) over a common universe U, we say that (f,A) is a soft subset of (g,B) if

(i) $A \subseteq B$

(ii) $f(e) \subseteq g(e)$ for $e \in A$.

Definition 2.3: [15] The extended *union* of two soft sets (f,A) and (g,B) over a common universe U is the soft set (h,C) where $C = A \cup B$ and $\forall e \in C$

$$h(e) = \begin{cases} f(e) & if\ e \in A - B \\ g(e) & if\ e \in B - A \\ f(e) \cup g(e) & if\ e \in A \cap B \end{cases}$$

We write $(f,A) \cup (g,B) = (h,C)$.

Definition 2.4: [15] The extended *intersection* of two soft sets (f,A) and (g,B) over a common universe U is the soft set (h,C) where $C = A \cup B$ and $\forall e \in C$

$$h(e) = \begin{cases} f(e) & if\ e \in A - B \\ g(e) & if\ e \in B - A \\ f(e) \cap g(e) & if\ e \in A \cap B \end{cases}$$

we write $(f,A) \cap (g,B) = (h,C)$.

Definition 2.5: [15] The complement of a soft set (f,A) is denoted by $(f,A)^{\tilde{c}}$ and is defined by $(f,A)^{\tilde{c}} = (f^c, A)$, where $f^c : A \to P(U)$ is a mapping defined by $f^c(e) = U - f(e)$ $for\ e \in A$.

Definition 2.6: [15] A soft set (f,A) is called a null soft set denoted by ϕ_{soft} if for all $e \in A, f(e) = \phi(\text{null set})$.

Definition 2.7: [15] A soft set (f,A) is called an absolute soft set denoted by U_{soft} if for all $e \in A, f(e) = U$.

Definition 2.8: [12] Let U,V be two universe sets and A,B be two sets of parameters Let $u: U \to V, p: A \to B$ be mappings. Then a mapping $f_{pu}: SS(U)_A \to SS(U)_B$ is defined as:

(i) let (g,A) be a soft set in $SS(U)_A$ Then the image of (g,A) under f_{pu}, denoted by $f_{pu}(g,A)$, is a soft set in $SS(U)_B$ defined by

$$f_{pu}(g,A), = \left(f_{pu}(g), p(A)\right), \text{ where for } y \in p(A),$$

$$f_{pu}(g)(y) = \begin{cases} \bigcup\limits_{x \in p^{-1}(y) \cap A} u\left(g(x)\right) & \text{if } p^{-1}(y) \cap A \neq \phi \\ \phi, \text{ otherwise} \end{cases}$$

(ii) let (h,B) be a soft set in $SS(U)_B$. Then the inverse image of (h,B) under f_{pu}, denoted by $f_{pu}^{-1}(h,B)$, is a soft set in $SS(U)_A$ defined by

$$f_{pu}^{-1}(h,B) = \left\langle f_{pu}^{-1}(h), p^{-1}(B)\right\rangle, \text{ where for } x \in A,$$

$$f_{pu}^{-1}(h)(x) = \begin{cases} u^{-1}\left(h\left(p(x)\right)\right) & \text{if } p(x) \in B \\ \phi, \text{ otherwise} \end{cases}$$

3. Refined Soft Sets

According to Molodtsov **[15]** a pair (f, A) is called a soft set over U, where A⊆E and f is a mapping given by f: A→ P(U). In this case f(a)⊆U for all a∈A. But there are many situations in real life problems in which f(a) is itself a soft set for each $a \in A$. Consider the following example:

Among thousands of paper submitted to a journal of Mathematical Science in a particular month, suppose the Editor initially selected 10 papers and forwarded them to two Reviewers to review those papers. Each of the Reviewers will review each paper depending upon the following parameters:

(i) originality of the paper
(ii) applications on real life problems
(iii) general interest on the topic chosen

The Editor will accept or reject a paper depending upon the review report of the Reviewers. *Let* $U=\{p_1, p_2, p_3, ..., p_{10}\}$ be the universe set of 10 papers. Let

$B=\{b_1(\textit{opinion of the 1st Reviewer}), b_2(\textit{opinion of the 2nd Reviewer})\}$,

$A=\{a_1(\text{originality of the paper}), a_2(\text{applications on real life problems}),$
$a_3(\text{general interest on the topic choosen})\}$.

Let $\zeta : B \to \hat{P}(A,U)$ (where $\hat{P}(A,U)$ denotes the collection of all soft sets over the universe set U) be defined by

$\zeta(b_1)=\{a_1=\{p_1, p_2, p_7, p_8\}, a_2=\{p_1, p_3, p_5, p_9\}, a_3=\{p_2, p_8, p_{10}\}\}$,

$\zeta(b_2)=\{a_1=\{p_2, p_7, p_8\}, a_2=\{p_1, p_5, p_9\}, a_3=\{p_8, p_{10}\}\}$.

Here (ζ, B) is not a traditional soft set. We call these type of sets as refined soft sets.

Definition 3.1: Let U be an universe set and E, F be two sets of parameters such that $E \cap F = \phi$. Let $A \subseteq E$ and $B \subseteq F$. Let us define a soft set (ζ, B) where $\zeta : B \to \hat{P}(A,U)$ is defined by $\zeta(b)=(f_b, A)$ for each $b \in B$ where (f_b, A) is a soft set over U for each $b \in B$. Then we say that (ζ, B) is a soft-soft set. We denote it by $\langle \zeta, B \rangle$.

Example 3.2: Consider the example that has been given in the beginning of the section-3. Then $\langle \zeta, B \rangle$ is a refined soft set.

Soft set theory basically deals with the opinion of one person depending on some parameters, whereas refined soft set theory deals with the opinion of several persons based on the common set of parameters which makes this theory more convenient and broadly applicable. When all the persons have same opinion, the corresponding refined soft set reduces to an ordinary soft set. Thus one can say that refined soft set is a generalization of traditional soft set. To illustrate this let us consider the following example:

Suppose Mr. X and his wife wants to jointly purchase a house depending upon the following parameters:

(i) Beautiful and cheap
(ii) Wooden

Let $U=\{h_1,h_2,h_3,h_4,h_5\}$ be the set of houses under consideration.

Let $B=\{b_1(\text{opinion of Mr. X}), b_2(\text{opinion of the wife of Mr. X})\}$, and

$A=\{a_1(\textit{beautiful and cheap}), a_2(\textit{wooden})\}$ be defined by

$\zeta(b_1)=\{a_1=\{h_1,h_2,h_4\}, a_2=\{h_1,h_5\}\}$, $\zeta(b_2)=\{a_1=\{h_1,h_2,h_4\}, a_2=\{h_1,h_5\}\}$.

Here (ζ,B) is an refined soft set. But since the opinion of Mr. X and his wife are same based on the same set of parameters, we conclude that (ζ,B) reduces to a soft set (g,A) where

$g(a_1)=\{h_1,h_2,h_4\}$, $g(a_2)=\{h_1,h_5\}$.

Thus we can say that soft set theory deals with collective decisions. On the other hand refined soft set theory deals with individual decisions.

Let U be a universe set and E, F be two sets of parameters such that $E\cap F=\phi$. Let $A\subseteq E$ and $B,C,D\subseteq F$. Let $\langle\zeta,B\rangle$, $\langle\xi,C\rangle$ and $\langle\varsigma,D\rangle$ be three refined soft sets over U, where $\zeta:B\to\hat{P}(A,U)$ is defined by $\zeta(b)=(f_b,A)$ for each $b\in B$; $\xi:C\to\hat{P}(A,U)$ is defined by $\xi(c)=(g_c,A)$ for each $c\in C$ and $\varsigma:D\to\hat{P}(A,U)$ is defined by $\varsigma(d)=(z_d,A)$ for each $d\in D$.

Definition 3.3: The *union* of $\langle\zeta,B\rangle$ and $\langle\xi,C\rangle$ is denoted by $\langle\zeta,B\rangle\tilde{\cup}\langle\xi,C\rangle$ and is defined by the refined soft set $\langle\omega,K\rangle$ where $K=B\cup C$ and $\omega:K\to\hat{P}(A,U)$ is given by

$$\omega(e)=\begin{cases}\zeta(e) & \textit{if } e\in B-C\\ \xi(e) & \textit{if } e\in C-B\\ \zeta(e)\cup\xi(e) & \textit{if } e\in B\cap C\end{cases}$$

Where $\zeta(e)\cup\xi(e)=(f_e,A)\cup(g_e,A)$

Definition 3.4: The *intersection* of $\langle \zeta, B\rangle$ and $\langle \xi, C\rangle$ is denoted by $\langle \zeta, B\rangle \tilde{\cap} \langle \xi, C\rangle$ and is defined by the refined soft set $\langle \vartheta, K\rangle$ where $K = B \cup C$ and $\vartheta : K \to \hat{P}(A,U)$ is given by

$$\vartheta(e) = \begin{cases} \zeta(e) & \text{if } e \in B - C \\ \xi(e) & \text{if } e \in C - B \\ \zeta(e) \cap \xi(e) & \text{if } e \in B \cap C \end{cases}$$

Where $\zeta(e) \cap \xi(e) = (f_e, A) \cap (g_e, A)$

Definition 3.5: The *complement* of $\langle \zeta, B\rangle$ is a refined soft set defined by $\langle \zeta, B\rangle^c$ and is defined by $\langle \zeta, B\rangle^c = \langle \zeta^c, B\rangle$ where $\zeta^c : B \to \hat{P}(A,U)$ is a mapping given by $\zeta^c(b) = (f_b^c, A)$ for $b \in B$ where $f_b^c : A \to \hat{P}(A,U)$ is a mapping defined by $f_b^c(a) = U - f_b(a)$ for $a \in A$.

Definition 3.7: A refined soft set $\langle \zeta, B\rangle$ is called a *null refined soft set* denoted by ϕ^* if $\zeta(b) = (f_b, A) = \phi_{soft}$ for each $b \in B$.

Definition 3.8: A refined soft set $\langle \zeta, B\rangle$ is called an *absolute refined soft set* denoted by U^* if $\zeta(b) = (f_b, A) = U_{soft}$ for each $b \in B$.

Theorem 3.9:

I. $\langle \zeta, B\rangle \tilde{\cup} \phi^* = \phi^* \tilde{\cup} \langle \zeta, B\rangle = \langle \zeta, B\rangle$ and $\langle \zeta, B\rangle \tilde{\cap} \phi^* = \phi^* \tilde{\cap} \langle \zeta, B\rangle = \phi^*$

II. $\langle \zeta, B\rangle \tilde{\cup} U^* = U^* \tilde{\cup} \langle \zeta, B\rangle = U^*$ and $\langle \zeta, B\rangle \tilde{\cap} U^* = U^* \tilde{\cap} \langle \zeta, B\rangle = \langle \zeta, B\rangle$

III. $\langle \zeta, B\rangle \tilde{\cup} \langle \xi, C\rangle = \langle \xi, C\rangle \tilde{\cup} \langle \zeta, B\rangle$

IV. $\langle \zeta, B\rangle \tilde{\cap} \langle \xi, C\rangle = \langle \xi, C\rangle \tilde{\cap} \langle \zeta, B\rangle$

V. $\langle \zeta, B\rangle \tilde{\cup} (\langle \xi, C\rangle \tilde{\cup} \langle \varsigma, D\rangle) = (\langle \zeta, B\rangle \tilde{\cup} \langle \xi, C\rangle) \tilde{\cup} \langle \varsigma, D\rangle$

VI. $\langle \zeta, B\rangle \tilde{\cap} (\langle \xi, C\rangle \tilde{\cap} \langle \varsigma, D\rangle) = (\langle \zeta, B\rangle \tilde{\cap} \langle \xi, C\rangle) \tilde{\cap} \langle \varsigma, D\rangle$

VII. $\langle \zeta, B\rangle \tilde{\cup} (\langle \xi, C\rangle \tilde{\cap} \langle \varsigma, D\rangle) = (\langle \zeta, B\rangle \tilde{\cup} \langle \xi, C\rangle) \tilde{\cap} (\langle \zeta, B\rangle \tilde{\cup} \langle \varsigma, D\rangle)$

VIII. $\langle \zeta, B\rangle \tilde{\cap} (\langle \xi, C\rangle \tilde{\cup} \langle \varsigma, D\rangle) = (\langle \zeta, B\rangle \tilde{\cap} \langle \xi, C\rangle) \tilde{\cup} (\langle \zeta, B\rangle \tilde{\cap} \langle \varsigma, D\rangle)$

IX. $(\langle \zeta, B\rangle \tilde{\cup} \langle \xi, C\rangle)^c = \langle \zeta, B\rangle^c \tilde{\cap} \langle \xi, C\rangle^c$

X. $(\langle \zeta, B\rangle \tilde{\cap} \langle \xi, C\rangle)^c = \langle \zeta, B\rangle^c \tilde{\cup} \langle \xi, C\rangle^c$

4. Operations between Refined Soft Sets and Soft Sets

Let us consider U as a universe set and E , F be two sets of parameters such that $E \cap F = \phi$. Let $A \subseteq E$ and $B, C \subseteq F$. Let us consider a refined soft set $\langle \zeta, B \rangle$ where $\zeta : B \to \hat{P}(A, U)$ is defined by $\zeta(b) = (f_b, A)$ for each $b \in B$. Let (g, B) be a soft set over U. Then

Definition 4.1:
(i) The operation "$\langle \zeta, B \rangle$ necessary(g, B) " denoted by $\langle \zeta, B \rangle \square (g, B)$ is defined by the soft refined set $\langle \zeta, B \rangle \square (g, B) = (\upsilon, B)$ *where* for $b \in B$, $\upsilon(\hat{b}) = \bigcap_{a \in A} \left(\left(U - f_b(a) \right) \cup g(b) \right)$
(ii) The operation "$\langle \zeta, B \rangle$ possibility(g, B) " denoted by $\langle \zeta, B \rangle \Diamond (g, B)$ is defined by the refined soft set $\langle \zeta, B \rangle \Diamond (g, B) = \langle \psi, B \rangle$ *where* for $b \in B$, $\psi(b) = \bigcup_{a \in A} \left(f_b(a) \cap g(b) \right)$

Theorem 4.2: Let (g_1, B) *and* (g_2, B) be two soft sets over U. Then
(i) $\langle \zeta, B \rangle \square U_{soft} = U_{soft}$ *and* $\langle \zeta, B \rangle \Diamond \phi_{soft} = \phi_{soft}$
(ii) $\langle \zeta, B \rangle \square (g_1, B) \subseteq (g, B) \subseteq \langle \zeta, B \rangle \Diamond (g_1, B)$
(iii) $(g_1, B) \tilde{\subseteq} (g_2, B) \Rightarrow \langle \zeta, B \rangle \square (g_1, B) \tilde{\subseteq} \langle \zeta, B \rangle \square (g_2, B)$
(iv) $(g_1, B) \tilde{\subseteq} (g_2, B) \Rightarrow \langle \zeta, B \rangle \Diamond (g_1, B) \tilde{\subseteq} \langle \zeta, B \rangle \Diamond (g_2, B)$
(v) $\langle \zeta, B \rangle \square \left((g_1, B) \cap (g_2, B) \right) = \left(\langle \zeta, B \rangle \square (g_1, B) \right) \cap \left(\langle \zeta, B \rangle \square (g_2, B) \right)$
(vi) $\langle \zeta, B \rangle \square \left((g_1, B) \cup (g_2, B) \right) \supseteq \left(\langle \zeta, B \rangle \square (g_1, B) \right) \tilde{\cup} \left(\langle \zeta, B \rangle \square (g_2, B) \right)$
(vii) $\langle \zeta, B \rangle \Diamond \left((g_1, B) \cap (g_2, B) \right) \subseteq \left(\langle \zeta, B \rangle \Diamond (g_1, B) \right) \tilde{\cap} \left(\langle \zeta, B \rangle \Diamond (g_2, B) \right)$
(viii) $\langle \zeta, B \rangle \Diamond \left((g_1, B) \cup (g_2, B) \right) = \left(\langle \zeta, B \rangle \Diamond (g_1, B) \right) \tilde{\cup} \left(\langle \zeta, B \rangle \Diamond (g_2, B) \right)$
(ix) $\left(\langle \zeta, B \rangle \square (g_1, B) \right)^c = \langle \zeta, B \rangle \Diamond (g_1, B)^c$
(x) $\left(\langle \zeta, B \rangle \Diamond (g_1, B) \right)^c = \langle \zeta, B \rangle \square (g_1, B)^c$

Proof: (i)-(iv) are straight forward.

(v) Let $\langle \zeta, B \rangle \square \left((g_1, B) \cap (g_2, B) \right) = \left(\upsilon, \hat{B} \right)$. Then for $b \in B$, we have

$$\upsilon(b) = \bigcap_{a \in A} \left(\left(U - f_b(a) \right) \cup \left(g_1(b) \cap g_2(b) \right) \right)$$
$$= \bigcap_{a \in A} \left(\left(\left(U - f_b(a) \right) \cup g_1(b) \right) \cap \left(\left(U - f_b(a) \right) \cup g_2(b) \right) \right)$$

Again $\left(\langle\zeta,B\rangle\square(g_1,B)\right)\cap\left(\langle\zeta,B\rangle\square(g_2,B)\right)=(\upsilon_1,B)\cap(\upsilon_2,B)=(\upsilon_3,B)$ where for $b\in B$, we have

$$\begin{aligned}\upsilon_3(b)&=\upsilon_1(b)\cap\upsilon_2(b)\\&=\bigcap_{a\in A}\left(\left(\left(U-f_b(a)\right)\cup g_1(b)\right)\cap\bigcap_{a\in A}\left(\left(U-f_b(a)\right)\cup g_2(b)\right)\right)\\&=\bigcap_{a\in A}\left(\left(\left(U-f_b(a)\right)\cup g_1(b)\right)\cap\left(\left(U-f_b(a)\right)\cup g_2(b)\right)\right)\end{aligned}$$

Hence $\langle\zeta,B\rangle\square\left((g_1,B)\cap(g_2,B)\right)=\left(\langle\zeta,B\rangle\square(g_1,B)\right)\cap\left(\langle\zeta,B\rangle\square(g_2,B)\right)$.

(vi) Let $\langle\zeta,B\rangle\square\left((g_1,B)\cup(g_2,B)\right)=(\upsilon,B)$. Then for $b\in B$, we have

$$\begin{aligned}\upsilon(b)&=\bigcap_{a\in A}\left(\left(U-f_b(a)\right)\cup\left(g_1(b)\cup g_2(b)\right)\right)\\&=\bigcap_{a\in A}\left(\left(\left(U-f_b(a)\right)\cup g_1(b)\right)\cup\left(\left(U-f_b(a)\right)\cup g_2(b)\right)\right)\end{aligned}$$

Again $\left(\langle\zeta,B\rangle\square(g_1,B)\right)\cup\left(\langle\zeta,B\rangle\square(g_2,B)\right)=(\upsilon_1,B)\cup(\upsilon_2,B)=(\upsilon_3,B)$ where for $b\in B$, we have

$$\begin{aligned}\upsilon_3(b)&=\upsilon_1(b)\cup\upsilon_2(b)\\&=\bigcap_{a\in A}\left(\left(\left(U-f_b(a)\right)\cup g_1(b)\right)\cup\bigcap_{a\in A}\left(\left(U-f_b(a)\right)\cup g_2(b)\right)\right)\end{aligned}$$

Hence $\langle\zeta,B\rangle\square\left((g_1,B)\cap(g_2,B)\right)=\left(\langle\zeta,B\rangle\square(g_1,B)\right)\cap\left(\langle\zeta,B\rangle\square(g_2,B)\right)$.

Since $g_1(b)\subseteq g_1(b)\cup g_2(b)$ *and* $g_2(b)\subseteq g_1(b)\cup g_2(b)$, we have

$\bigcap_{a\in A}\left(\left(U-f_b(a)\right)\cup g_1(b)\right)\subseteq\bigcap_{a\in A}\left(\left(U-f_b(a)\right)\cup\left(g_1(b)\cup g_2(b)\right)\right)$ *and*

$\bigcap_{a\in A}\left(\left(U-f_b(a)\right)\cup g_2(b)\right)\subseteq\bigcap_{a\in A}\left(\left(U-f_b(a)\right)\cup\left(g_1(b)\cup g_2(b)\right)\right)$. Consequently,

$$\bigcap_{a\in A}\left(\left(U-f_b(a)\right)\cup g_1(b)\right)\cup\bigcap_{a\in A}\left(\left(U-f_b(a)\right)\cup g_2(b)\right)\subseteq\bigcap_{a\in A}\left(\left(U-f_b(a)\right)\cup\left(g_1(b)\cup g_2(b)\right)\right).$$

So $\langle\zeta,B\rangle\square\left((g_1,B)\cup(g_2,B)\right)\supseteq\left(\langle\zeta,B\rangle\square(g_1,B)\right)\tilde{\cup}\left(\langle\zeta,B\rangle\square(g_2,B)\right)$.

(vii)-(viii) can be proved similarly.

(ix) Let $\langle \zeta, B\rangle \Diamond (g_1, B)^c = \langle \psi, B\rangle$ *where* for $b \in B$, we have $\psi(b) = \bigcup_{a\in A}\left(f_b(a) \cap (U - g(b))\right)$

Again for $\left(\langle \zeta, B\rangle \Box (g_1, B)\right)^c = (\upsilon, B)$ and for $b \in B$, we have

$$\upsilon(b) = U - \left(\bigcap_{a\in A} \left((U - f_b(a)) \cup g(b)\right)\right)$$
$$= \bigcup_{a\in A}\left(f_b(a) \cap (U - g(b))\right)$$

Consequently, $\left(\langle \zeta, B\rangle \Box (g_1, B)\right)^c = \langle \zeta, B\rangle \Diamond (g_1, B)^c$.

(x) Proof is similar to (ix).

5. Soft Images and Soft Inverse Images of Refined Soft Sets

Definition 5.1: Let U, V be two universe sets and E_1, E_2, F_1, F_2 be four universe sets of parameters such that $E_i \cap F_j = \phi$ for $i, j = 1, 2.$. Let $A_1 \subseteq E_1$ and $A_2 \subseteq E_2$ and $B \subseteq F_1$ and $C \subseteq F_2$. Let $u : U \to V, p : B \to C$ *and* $q : A_1 \to A_2$ be mappings. Let $SS(U)_B^{A_1}$ and $SS(V)_C^{A_2}$ be two families of refined soft sets. Then a mapping $f_{qpu} : SS(U)_B^{A_1} \to SS(U)_C^{A_2}$ is defined as:

(i) Let $\langle \zeta, B\rangle$ be a refined soft set in $SS(U)_B^{A_1}$ and $\zeta(b) = (r_b, A_1)$ for each $b \in B$. Then the image of $\langle \zeta, B\rangle$ under f_{qpu}, denoted by $f_{q\bar{p}u}\langle \zeta, B\rangle$, is a refined soft set in $SS(U)_C^{A_2}$ defined by $f_{qpu}\langle \zeta, B\rangle = \langle f_{qpu}(\zeta), p(B)\rangle$, where for $c \in p(B)$, $f_{qpu}(\zeta)(c) = (z_c, A_2)$ where for $a^{//} \in A_2$

$$z_c(a^{//}) = \begin{cases} \bigcup_{c^{/} \in p^{-1}(c)\cap B} \left[\bigcup_{a^{/} \in q^{-1}(a^{//})\cap A_1} u\left(r_{c^{/}}(a^{/})\right)\right] & \text{if } p^{-1}(c) \cap B \neq \phi \text{ and } q^{-1}(a^{//}) \cap A_1 \neq \phi \\ \phi, \text{ otherwise} \end{cases}$$

(ii) Let $\langle \varsigma, C\rangle$ be a refined soft set in $SS(U)_C^{A_2}$ and $\varsigma(c) = (k_c, A_2)$ for each $c \in C$. Then the inverse image of $\langle \varsigma, C\rangle$ under f_{qpu}, denoted by $f_{qpu}^{-1}\langle \varsigma, C\rangle$, is a refined soft set in $SS(U)_B^{A_1}$ defined by

$f_{qpu}^{-1}\langle \varsigma, C\rangle = \langle f_{qpu}^{-1}(\varsigma), p^{-1}(C)\rangle$, where for $b \in p^{-1}(C)$, $f_{qpu}^{-1}(\varsigma)(b) = (t_b, A_1)$ where for

$$a^{/} \in A_1,\ t_b\left(a^{/}\right)=\begin{cases} u^{-1}\left(k_{p(b)}\left(q\left(a^{/}\right)\right)\right) \text{ if } p(b)\neq\phi \\ \phi, \text{ otherwise} \end{cases}$$

The refined soft function f_{qpu} is called surjective if p, q, u are all surjective. The refined soft function f_{qpu} is called injective if p, q, u are all injective.

Example 5.2: Let $U=\{h_1,h_2,h_3,h_4,h_5,h_6\}$, $V=\{v_1,v_2,v_3\}$ and $u:U\to V$ be defined by

$u(h_1)=v_1, u(h_2)=v_3, u(h_3)=v_3, u(h_4)=v_1, u(h_5)=v_2, u(h_1)=v_1.$

Let $B=\{b_1,b_2\}$, $B=\{c_1,c_2\}$ and $p:B\to C$ be defined by $p(b_1)=c_1, p(b_2)=c_1.$

Let $A_1=\{\alpha_1,\alpha_2,\alpha_3\}$, $A_2=\{\beta_1,\beta_2,\beta_3\}$ *and* $q:A_1\to A_2$ be defined by

$q(\alpha_1)=\beta_1, q(\alpha_2)=\beta_1, q(\alpha_3)=\beta_2.$

$p(B)=\{p(b):b\in B\}=\{c_1\}$ and so $c\in p(B)\Rightarrow c=c_1$ *and* $p^{-1}(c)=p^{-1}(c_1)=\{b_1,b_2\}.$

Let $r_{b_1}(\alpha_1)=\{h_1,h_2,h_4\}$, $r_{b_1}(\alpha_2)=\{h_1,h_3,h_5\}$, $r_{b_1}(\alpha_3)=\{h_2,h_3,h_6\}$,
$r_{b_2}(\alpha_1)=\{h_1,h_3,h_4,h_6\}$, $r_{b_2}(\alpha_2)=\{h_3,h_4,h_5\}$ and $r_{b_2}(\alpha_3)=\{h_2,h_5\}.$

Here $a^{//}\in A_2=\{\beta_1,\beta_2,\beta_3\}.$
$z_c(\beta_1)=u\left(r_{b_1}(\alpha_1)\right)\cup u\left(r_{b_1}(\alpha_2)\right)=u\left(\{h_1,h_2,h_4\}\right)\cup u\left(\{h_1,h_3,h_5\}\right)=\{v_1,v_3\}\cup\{v_1,v_2,v_3\}=\{v_1,v_2,v_3\},$
$z_c(\beta_2)=u\left(r_{b_1}(\alpha_3)\right)\cup u\left(r_{b_2}(\alpha_3)\right)=u\left(\{h_2,h_3,h_6\}\right)\cup u\left(\{h_2,h_5\}\right)=\{v_1,v_3\}\cup\{v_1,v_2,v_3\}=\{v_1,v_2,v_3\},$
$z_c(\beta_3)=\{\ \}.$

Hence $f_{qpu}\langle\zeta,B\rangle=\{c_1=\{\beta_1=\{v_1,v_2,v_3\},\ \beta_2=\{v_1,v_2,v_3\},\ \beta_3=\{\ \}\}\}.$
$p^{-1}(C)=\{b_1,b_2\}.$

Let $k_{c_1}(\beta_1)=\{v_1,v_2\}$, $k_{c_1}(\beta_2)=\{v_3\}$, $k_{c_1}(\beta_3)=\{v_1,v_3\}$, $k_{c_2}(\beta_1)=\{v_2\}$, $k_{c_2}(\beta_2)=\{v_2,v_3\}$
and $k_{c_2}(\beta_3)=\{v_1,v_2,v_3\}.$
Then $t_{b_1}(\alpha_1)=u^{-1}\left(k_{c_1}\left(q(\alpha_1)\right)\right)=u^{-1}\left(k_{c_1}(\beta_1)\right)=u^{-1}\left(\{v_1,v_2\}\right)=\{h_1,h_4,h_5,h_6\},$
$t_{b_1}(\alpha_2)=u^{-1}\left(k_{c_1}\left(q(\alpha_2)\right)\right)=u^{-1}\left(k_{c_1}(\beta_1)\right)=u^{-1}\left(\{v_1,v_2\}\right)=\{h_1,h_4,h_5,h_6\},$

$$t_{b_1}(\alpha_3)=u^{-1}\left(k_{c_1}\left(q(\alpha_3)\right)\right)=u^{-1}\left(k_{c_1}(\beta_2)\right)=u^{-1}\left(\{v_3\}\right)=\{h_2,h_3\},$$
$$t_{b_2}(\alpha_1)=u^{-1}\left(k_{c_1}\left(q(\alpha_1)\right)\right)=u^{-1}\left(k_{c_1}(\beta_1)\right)=u^{-1}\left(\{v_1,v_2\}\right)=\{h_1,h_4,h_5,h_6\},$$
$$t_{b_2}(\alpha_2)=u^{-1}\left(k_{c_1}\left(q(\alpha_2)\right)\right)=u^{-1}\left(k_{c_1}(\beta_1)\right)=u^{-1}\left(\{v_1,v_2\}\right)=\{h_1,h_4,h_5,h_6\},$$
$$t_{b_2}(\alpha_3)=u^{-1}\left(k_{c_1}\left(q(\alpha_3)\right)\right)=u^{-1}\left(k_{c_1}(\beta_2)\right)=u^{-1}\left(\{v_3\}\right)=\{h_2,h_3\}.$$

Hence $f_{qpu}{}^{-1}\langle\varsigma,C\rangle=\{b_1=\{\alpha_1=\alpha_2=\{h_1,h_4,h_5,h_6\},\alpha_3=\{h_2,h_3\}\},$
$b_2=\{\alpha_1=\alpha_2=\{h_1,h_4,h_5,h_6\},\alpha_3=\{h_2,h_3\}\}\}.$

6. Application

The concept of image of a refined soft set can be used in a customer query problem. Suppose the following is a narration by a customer to a shopkeeper:

"I mainly need an android smart phone with long battery life and minimum 1GB of RAM. There should be 3G type network connectivity in the mobile. The rear and front camera should be a minimum of 5MP and 2MP respectively. Can you please give me some idea about the cost and the OS version of a smart phone which has 4.8 inch or 5 inch display size?"

According to the demand of the customer and based on the availability of the smart phones in the shop, let us consider the following refined soft set on the universe of smart phones $U=\{m_1, m_2, m_3, \ldots, m_{10}\}$:

$$\langle g,B\rangle=\begin{cases}\text{battery}(b_1)=\begin{cases}\text{high importance}(a_1)=\{m_1,m_2,m_7\}\\ \text{medium importance}(a_2)=\{m_4,m_5,m_6\}\\ \text{low importance}(a_3)=\{m_3,m_8,m_9,m_{10}\}\end{cases}\\ \text{camera}(b_2)=\begin{cases}\text{high importance}(a_1)=\{m_1,m_4,m_6\}\\ \text{medium importance}(a_2)=\{m_2,m_3,m_8\}\\ \text{low importance}(a_3)=\{m_5,m_7,m_9,m_{10}\}\end{cases}\end{cases}$$

where $B=\{b_1,b_2\}$ and let $A=\{a_1,a_2,a_3\}$. Let $V=\{o_1$ (*jellybean*), o_2 (*kitkat*), o_3 (*lollipop*)$\}$ be the set of android versions; $A_2=\{a_1''$ (*high cost* (*more than 10,000*)), a_1'' (*medium cost* (*between 7000-10,000*)), a_1'' (*low cost* (*less than 7000*))$\}$; $C=\{c_1$ (*display size is 4.8 inch*), c_2 (*display size is 5 inch*)$\}$.

Let $u:U\to V$ be defined by $u(m_1)=u(m_3)=u(m_9)=o_1$, $u(m_2)=u(m_5)=u(m_7)=o_2$, $u(m_4)=u(m_6)=u(m_8)=u(m_{10})=o_3$. Let $p:B\to C$ be defined by $p(b_1)=c_1$, $p(b_2)=c_2$. Let

$q:A_1\to A_2$ be defined by $q(a_1)=a_3''$, $q(a_2)=a_2''$ $q(a_3)=a_1''$.

Then $p(B)=\{p(b):b\in B\}=\{c_1,c_2\}$.

Now $f_{qpu}(\langle g,B\rangle)=\langle f_{qpu},p(B)\rangle$.

where for $c\in p(B)$, $f_{qpu}(C)=(Z_c,A_2)$,

where for $a''\in A_2$, $Z_c(a'')=\bigcup_{c'\in p^{-1}(c)\cap B}\ \bigcup_{a'\in q^{-1}(a'')\cap A_1} u(r_{c'}(a'))$

So

$$\begin{aligned}Z_{c_1}(a_1'')&=\bigcup_{c'\in\{b_1\}}\ \bigcup_{a'\in\{a_3\}} u(r_{c'}(a'))\\&=u(r_{b_1}(a_3))\\&=u(\{m_3,m_8,m_9,m_{10}\})\\&=\{o_1,o_3\}\end{aligned}$$

$$\begin{aligned}Z_{c_1}(a_2'')&=\bigcup_{c'\in\{b_1\}}\ \bigcup_{a'\in\{a_2\}} u(r_{c'}(a'))\\&=u(r_{b_1}(a_2))\\&=u(\{m_4,m_5,m_6\})\\&=\{o_2,o_3\}\end{aligned}$$

$$\begin{aligned}Z_{c_1}(a_3'')&=\bigcup_{c'\in\{b_1\}}\ \bigcup_{a'\in\{a_1\}} u(r_{c'}(a'))\\&=u(r_{b_1}(a_1))\\&=u(\{m_1,m_2,m_7\})\\&=\{o_1,o_2\}\end{aligned}$$

$$\begin{aligned}Z_{c_2}(a_1'')&=\bigcup_{c'\in\{b_2\}}\ \bigcup_{a'\in\{a_3\}} u(r_{c'}(a'))\\&=u(r_{b_2}(a_3))\\&=u(\{m_5,m_7,m_9,m_{10}\})\\&=\{o_1,o_2,o_3\}\end{aligned}$$

$$Z_{c_2}\left(a_2''\right)=\bigcup_{c'\in\{b_2\}}\bigcup_{a'\in\{a_2\}}u\left(r_{c'}\left(a'\right)\right)$$
$$=u\left(r_{b_2}\left(a_2\right)\right)$$
$$=u\left(\left\{m_2,m_3,m_8\right\}\right)$$
$$=\left\{o_1,o_2,o_3\right\}$$

$$Z_{c_2}\left(a_3''\right)=\bigcup_{c'\in\{b_2\}}\bigcup_{a'\in\{a_1\}}u\left(r_{c'}\left(a'\right)\right)$$
$$=u\left(r_{b_2}\left(a_1\right)\right)$$
$$=u\left(\left\{m_1,m_4,m_6\right\}\right)$$
$$=\left\{o_1,o_3\right\}$$

Thus

$$f_{qpu}\left(\langle g,B\rangle\right)=\begin{cases}c_1=\begin{cases}a_1''=\left\{o_1,o_3\right\}\\a_2''=\left\{o_2,o_3\right\}\\a_3''=\left\{o_1,o_2\right\}\end{cases}\\c_2=\begin{cases}a_1''=\left\{o_1,o_2,o_3\right\}\\a_2''=\left\{o_1,o_2,o_3\right\}\\a_3''=\left\{o_1,o_3\right\}\end{cases}\end{cases}$$
$$=\begin{cases}display\ size\ is\ 4.8\ inch=\begin{cases}high\ cost=\left\{o_1,o_3\right\}\\medium\ cost=\left\{o_2,o_3\right\}\\low\ cost=\left\{o_1,o_2\right\}\end{cases}\\display\ size\ is\ 5\ inch=\begin{cases}high\ cost=\left\{o_1,o_2,o_3\right\}\\medium\ cost=\left\{o_1,o_2,o_3\right\}\\low\ cost=\left\{o_1,o_3\right\}\end{cases}\end{cases}$$

Thus

(i) Considering the display size 4.8 inch and high cost, the preferred operating systems are o_1 and o_3.

(ii) Considering the display size 4.8 inch and medium cost, the preferred operating systems are o_2 and o_3.

(iii) Considering the display size 4.8 inch and low cost, the preferred operating systems are o_1 and o_2.

(iv) Considering the display size 5 inch and high cost, the preferred operating systems are o_1, o_2 and o_3.

(v) Considering the display size 5 inch and medium cost, the preferred operating systems are o_1, o_2 and o_3.

(vi) Considering the display size 5 inch and low cost, the preferred operating systems are o_1 and o_3.

7. Conclusion and Future Works

Soft set theory is a general method for solving problem of uncertainty. In the present paper the structure of refined soft set is discussed together with their operations and basic properties. Moreover the concept of soft image and soft inverse image in refined soft set theory context are presented which may be useful in medical expert system.

With the motivation of ideas presented in this paper one can think of similarity measures, Cartesian products and relations on refined soft sets. Further studies on the topology generated by the refined soft sets or refined soft set relations may be done so that we may brood over the topological side of refined soft sets or refined soft set relations. Moreover the refined soft sets and the refined soft set relations can be extended in fuzzy refined soft sets and fuzzy refined soft set relations respectively and thus one can get more affirmative solution in decision making problems in real life situations. It is hoped that the combinations of refined soft sets, fuzzy sets and rough sets will generate potentially interesting some new research direction.

References

[1] H. Aktas, N. Cagman, Soft sets and soft groups, Information Sciences 177(13) (2007) 2726-2735.

[2] M. I. Ali, F. Feng, X. Liu, W. K. Min, M. Shabir, On some new operations in soft set theory, Computers and Mathematics with Applications 57 (2009) 1547-1553.

[3] K. Atanassov, Intuitionistic fuzzy sets, Fuzzy Sets and Systems 20 (1986) 87-96.

[4] K. Atanassov, Operators over interval valued intuitionistic fuzzy sets, Fuzzy Sets and Systems 64 (1994) 159-174.

[5] K. V. Babitha and J.J Sunil, Soft set relations and functions, Computers and Mathematics with Applications 60 (2010) 1840-1849.

[6] D. Chen, E.C.C. Tsang, D. S. Yeung, X. Wang, The parameterization reduction of soft Sets and its applications, Computers and Mathematics with Applications 49 (2005) 757-763.

[7] F. Feng, Y. B. Jun, X. Zhao, Soft semi rings, Computers and Mathematics with Applications 56(2008) 2621-2628.

[8] W. L. Gau and D. J. Buehrer, Vague sets, IEEE Trans. System Man Cybernet 23 (2) (1993) 610-614.

[9] M. B. Gorzalzany, A method of inference in approximate reasoning based on interval valued fuzzy sets, Fuzzy Sets and Systems 21 (1987) 1-17.

[10] Y. B. Jun, Soft BCK/BCI-algebras, Computers and Mathematics with Applications 56 (2008) 1408-1413.
[11] Y. B. Jun, C.H. Park, Applications of soft sets in ideal theory of BCK/BCI algebras, Information Sciences 178 (2008) 2466-2475.
[12] A. Kharal, B. Ahmad; The Mappings on soft classes, New Mathematics and Natural Computation 7(3) (2011) 471-481.
[13] Z. Kong, L. Gao, L. Wang, S. Li, The normal parameter reduction of soft sets and its algorithm, Computers and Mathematics with Applications 56(2008) 3029-3037.
[14] P. K. Maji, R. Biswas, A. R. Roy, Soft set theory, Computers and Mathematics with Applications 45 (2003) 555-562.
[15] D. Molodtsov, Soft set theory-first results, Computers and Mathematics with Applications 37 (1999) 19-31.
[16] Z. Pawlak, Rough sets, International Journal of Computing and Information Sciences 11 (1982) 341-356.
[17] K.Y.Qin, Z. Y. Hong, On soft equality, Journal of Computational and Applied Mathematics 234 (2010) 1347-1355.
[18] L.A. Zadeh, Fuzzy sets, Information and Control 8 (1965) 338-353.

http://www.newtheory.org **ISSN: 2149-1402**

Journal of New Theory

Received: 20.06.2016 *Year*: **2016**, *Number*: **14**, *Pages*: **26-36**
Published: 14.07.2016 *Original Article*[**]

SOME GENERALIZATIONS OF THE BANACH'S CONTRACTION PRINCIPLE ON A COMPLETE COMPLEX VALUED S-METRIC SPACE

Nihal Yılmaz Özgür <nihal@balikesir.edu.tr>
Nihal Taş[*] <nihaltas@balikesir.edu.tr>

Department of Mathematics, University of Balıkesir, 10145 Balıkesir, Turkey

Abstract — In this paper we give some generalizations of the Banach's contraction principle on a complete complex valued S-metric space. We verify our results with an example.

Keywords — *Complex valued S-metric space, Fixed point, Banach's contraction principle.*

1 Introduction

Metric spaces and fixed-point theory have an important role in various areas of mathematics such as analysis, topology, differential equation etc. Fixed-point theory begin with the Banach's contraction principle. Then the principle has been studied and generalized on some metric spaces (see [1], [2], [6], [7] and [8]). Recently, it has been introduced the notion of an S-metric space as a generalization of a metric space [8]. Some mathematicans proved new fixed-point theorems on an S-metric space (see [4], [5], [6], [8], [9] and [10]). Mlaiki presented the concept of a complex valued S-metric space and gave a common fixed-point theorem of two self-mappings on a complex valued S-metric space [3]. The present authors investigated new common fixed-point theorems using the notion of CS-compatibility on a complex valued S-metric space [7].

Let $X = \mathbb{C}$ and the function $S : \mathbb{C} \times \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ be defined by

$$S(x, y, z) = i\left(|x - z| + |y - z|\right),$$

[**] *Edited by* Oktay Muhtaroğlu *(Area Editor) and* Naim Çağman *(Editor-in-Chief).*
[*] *Corresponding Author.*

for all $x, y, z \in \mathbb{C}$. Then the function S is a complex valued S-metric space on $\mathbb{C}$. Let us define the self-mapping $T : \mathbb{C} \to \mathbb{C}$ as follows:

$$Tx = 1 - x,$$

for all $x \in \mathbb{C}$. Then T is a self-mapping on the complete complex valued S-metric space $(\mathbb{C}, S)$. T has a fixed point $x = \frac{1}{2}$, but it does not satisfy the condition of Banach's contraction principle. Therefore it is important to study new generalized fixed-point theorems.

Motivated by the above studies, in this paper, we investigate new fixed-point theorems as generalizations of the Banach's contraction principle on a complete complex valued S-metric spaces. We expect that new generalized fixed-point theorems will be obtained using our main theorems.

In Section 2 we recall some known definitions, lemmas and a theorem. In Section 3 we generalize the Banach's contraction principle on a complete complex valued S-metric space. Also we give an example which satisfies the conditions of our results, but does not satisfy the condition of Banach's contraction principle.

2 Preliminary

In this section we recall some definitions, lemmas and a theorem which is called the Banach's contraction principle.

Let $\mathbb{C}$ be the set of complex numbers and z_1, $z_2 \in \mathbb{C}$. The partial order $\precsim$ is defined on $\mathbb{C}$ as follows:

$$z_1 \precsim z_2 \text{ if and only if } Re(z_1) \leq Re(z_2),\ Im(z_1) \leq Im(z_2)$$

and

$$z_1 \prec z_2 \text{ if and only if } Re(z_1) < Re(z_2),\ Im(z_1) < Im(z_2).$$

Also we write $z_1 \precsim z_2$ if one of the following conditions hold:

1. $Re(z_1) = Re(z_2)$ and $Im(z_1) < Im(z_2)$,
2. $Re(z_1) < Re(z_2)$ and $Im(z_1) = Im(z_2)$,
3. $Re(z_1) = Re(z_2)$ and $Im(z_1) = Im(z_2)$.

Note that

$$0 \precsim z_1 \precsim z_2 \Rightarrow |z_1| < |z_2|$$

and

$$z_1 \precsim z_2,\ z_2 \prec z_3 \Rightarrow z_1 \prec z_3.$$

Definition 2.1. [3] Let X be a nonempty set. A complex valued S-metric on X is a function $S : X \times X \times X \to \mathbb{C}$ that satisfies the following conditions for all $x, y, z, t \in X$:

(**CS1**) $0 \precsim S(x, y, z)$,

(**CS2**) $S(x, y, z) = 0$ if and only if $x = y = z$,

(**CS3**) $S(x, y, z) \precsim S(x, x, t) + S(y, y, t) + S(z, z, t)$.

The pair (X, S) is called a complex valued S-metric space.

Definition 2.2. [3] Let (X, S) be a complex valued S-metric space. Then

1. A sequence $\{a_n\}$ in X converges to x if and only if for all ε such that $0 \prec \varepsilon \in \mathbb{C}$ there exists a natural number n_0 such that for all $n \geq n_0$, we have $S(a_n, a_n, x) \prec \varepsilon$ and it is denoted by
$$\lim_{n\to\infty} a_n = x.$$

2. A sequence $\{a_n\}$ in X is called a Cauchy sequence if for all ε such that $0 \prec \varepsilon \in \mathbb{C}$ there exists a natural number n_0 such that for all $n, m \geq n_0$, we have $S(a_n, a_n, a_m) \prec \varepsilon$.

3. A complex valued S-metric space (X, S) is called complete if every Cauchy sequence is convergent.

Lemma 2.3. [3] Let (X, S) be a complex valued S-metric space and $\{a_n\}$ be a sequence in X. Then $\{a_n\}$ converges to x if and only if
$$|S(a_n, a_n, x)| \to 0,$$
as $n \to \infty$.

Lemma 2.4. [3] Let (X, S) be a complex valued S-metric space and $\{a_n\}$ be a sequence in X. Then $\{a_n\}$ is a Cauchy sequence if and only if
$$|S(a_n, a_n, a_m)| \to 0,$$
as $n \to \infty$.

Lemma 2.5. [3] If (X, S) be a complex valued S-metric space then
$$S(x, x, y) = S(y, y, x),$$
for all $x, y \in X$.

Lemma 2.6. [9] Let $(X, S), (Y, S')$ be two S-metric spaces and $f : X \to Y$ be a function. Then f is continuous at $x \in X$ if and only if $f(x_n) \to f(x)$ whenever $x_n \to x$.

In the next section, we consider two complex valued S-metric spaces in Lemma 2.6.

Now we recall the following theorem which is called the Banach's contraction principle.

Theorem 2.7. [7] Let (X, S) be a complete complex valued S-metric space and T be a self-mapping of X satisfying

$$S(Tx, Tx, Ty) \precsim hS(x, x, y) \tag{1}$$

for all $x, y \in X$ and some $0 \leq h < 1$. Then f has a fixed point in X.

3 Main Results

In this section we prove new generalizations of the Banach's contraction principle.

Theorem 3.1. Let (X, S) be a complete complex valued S-metric space and T be a self-mapping of X. If there exist nonnegative real numbers c_1, c_2, c_3, c_4 satisfying $\max\{c_1 + 3c_3 + 2c_4, c_1 + c_2 + c_3, c_2 + 2c_4\} < 1$ such that

$$\begin{aligned} S(Tx, Tx, Ty) \preceq\ & c_1 S(x, x, y) + c_2 S(Tx, Tx, y) + c_3 S(Ty, Ty, x) \\ & + c_4 \max\{S(Tx, Tx, x), S(Ty, Ty, y)\}, \end{aligned} \tag{2}$$

for all $x, y \in X$, then T has a unique fixed point x in X and T is continuous at x.

Proof. Let $a_0 \in X$ and the sequence $\{a_n\}$ be defined by

$$T^n a_0 = a_n.$$

Assume that $a_n \neq a_{n+1}$ for all n. Using the inequality 2 we obtain

$$\begin{aligned} S(a_n, a_n, a_{n+1}) &= S(Ta_{n-1}, Ta_{n-1}, Ta_n) \preceq c_1 S(a_{n-1}, a_{n-1}, a_n) \\ &\quad + c_2 S(a_n, a_n, a_n) + c_3 S(a_{n+1}, a_{n+1}, a_{n-1}) \\ &\quad + c_4 \max\{S(a_n, a_n, a_{n-1}), S(a_{n+1}, a_{n+1}, a_n)\} \\ &= c_1 S(a_{n-1}, a_{n-1}, a_n) + c_3 S(a_{n+1}, a_{n+1}, a_{n-1}) \\ &\quad + c_4 \max\{S(a_n, a_n, a_{n-1}), S(a_{n+1}, a_{n+1}, a_n)\}. \end{aligned} \tag{3}$$

Using the condition $(CS3)$, we get

$$S(a_{n+1}, a_{n+1}, a_{n-1}) \preceq 2S(a_{n+1}, a_{n+1}, a_n) + S(a_{n-1}, a_{n-1}, a_n). \tag{4}$$

Hence using the inequalities (3), (4) and Lemma 2.5, we have

$$S(a_n, a_n, a_{n+1}) \preceq c_1 S(a_{n-1}, a_{n-1}, a_n) + 2c_3 S(a_{n+1}, a_{n+1}, a_n) + c_3 S(a_{n-1}, a_{n-1}, a_n)$$

$$+c_4S(a_n,a_n,a_{n-1})+c_4S(a_{n+1},a_{n+1},a_n),$$
$$(1-2c_3-c_4)S(a_n,a_n,a_{n+1})\preceq(c_1+c_3+c_4)S(a_{n-1},a_{n-1},a_n)$$

and

$$S(a_n,a_n,a_{n+1})\preceq\frac{c_1+c_3+c_4}{1-2c_3-c_4}S(a_{n-1},a_{n-1},a_n). \tag{5}$$

Let $c=\frac{c_1+c_3+c_4}{1-2c_3-c_4}$. Then we find $c<1$ since $c_1+3c_3+2c_4<1$. Using the inequality (5), we obtain

$$S(a_n,a_n,a_{n+1})\preceq c^nS(a_0,a_0,a_1). \tag{6}$$

For all $n,m\in\mathbb{N}$, $n<m$, using the inequality (6) and the condition $(CS3)$, we have

$$\begin{aligned}
S(a_n,a_n,a_m) &\preceq 2S(a_n,a_n,a_{n+1})+2S(a_{n+1},a_{n+1},a_{n+2})+\cdots+2S(a_{m-1},a_{m-1},a_m)\\
&\preceq 2(c^n+c^{n+1}+\cdots+c^{m-1})S(a_0,a_0,a_1)\\
&\preceq 2c^n(1+c+\cdots+c^{m-n-1})S(a_0,a_0,a_1)\\
&\preceq 2c^n\frac{1-c^{m-n}}{1-c}S(a_0,a_0,a_1)\\
&\preceq \frac{2c^n}{1-c}S(a_0,a_0,a_1),
\end{aligned}$$

which implies

$$|S(a_n,a_n,a_m)|\leq\frac{2c^n}{1-c}\left|S(a_0,a_0,a_1)\right|.$$

Therefore $|S(a_n,a_n,a_m)|\to 0$ as $n,m\to\infty$. Hence $\{a_n\}$ is a Cauchy sequence. Since (X,S) is complete, there exists $x\in X$ such that $\{a_n\}$ converges to x.

Now we show that x is a fixed point of T. Suppose that $Tx\neq x$. Then we get

$$\begin{aligned}
S(a_n,a_n,Tx) &= S(Ta_{n-1},Ta_{n-1},Tx)\preceq c_1S(a_{n-1},a_{n-1},x)\\
&\quad +c_2S(a_n,a_n,x)+c_3S(Tx,Tx,a_{n-1})\\
&\quad +c_4\max\{S(a_n,a_n,a_{n-1}),S(Tx,Tx,x)\}
\end{aligned}$$

and

$$\begin{aligned}
|S(a_n,a_n,Tx)| &\leq c_1\left|S(a_{n-1},a_{n-1},x)\right|+c_2\left|S(a_n,a_n,x)\right|+c_3\left|S(Tx,Tx,a_{n-1})\right|\\
&\quad +c_4\left|\max\{S(a_n,a_n,a_{n-1}),S(Tx,Tx,x)\}\right|.
\end{aligned}$$

If we take limit for $n\to\infty$, then using the continuity of S and Lemma 2.5, we have

$$|S(x,x,Tx)|=|S(Tx,Tx,x)|\leq(c_3+c_4)\left|S(Tx,Tx,x)\right|,$$

which is a contradiction since $0\leq c_3+c_4<1$. Hence we obtain $Tx=x$.

Now we show that x is unique. Let y be another fixed point of T such that $x\neq y$. Using the inequality (2) and Lemma 2.5, we have

$$\begin{aligned}
S(Tx,Tx,Ty) &= S(x,x,y)\preceq c_1S(x,x,y)+c_2S(x,x,y)\\
&\quad +c_3S(y,y,x)+c_4\max\{S(x,x,x),S(y,y,y)\}
\end{aligned}$$

and

$$|S(x,x,y)| \leq (c_1+c_2+c_3)\,|S(x,x,y)|\,,$$

which implies $x=y$ since $c_1+c_2+c_3<1$.

Now we prove that T is continuous at x. For $n\in\mathbb{N}$, using the inequality (2), we get

$$\begin{aligned} S(Ta_n,Ta_n,Tx) &\preceq c_1S(a_n,a_n,x)+c_2S(Ta_n,Ta_n,x) \\ &\quad +c_3S(Tx,Tx,a_n)+c_4\max\{S(Ta_n,Ta_n,a_n),S(Tx,Tx,x)\}. \end{aligned} \tag{7}$$

Using the condition $(CS3)$, the inequality (7) and Lemma 2.5, we obtain

$$\begin{aligned} S(Ta_n,Ta_n,Tx) &\preceq c_1S(a_n,a_n,x)+c_2S(Ta_n,Ta_n,x)+c_3S(Tx,Tx,a_n) \\ &\quad +2c_4S(Ta_n,Ta_n,x)+c_4S(a_n,a_n,x) \end{aligned}$$

and

$$(1-c_2-2c_4)S(Ta_n,Ta_n,Tx)\preceq(c_1+c_3+c_4)S(a_n,a_n,x),$$

which implies

$$|S(Ta_n,Ta_n,Tx)|\leq\frac{c_1+c_3+c_4}{1-c_2-2c_4}\,|S(a_n,a_n,x)|\,.$$

If we take limit for $n\to\infty$, then we have

$$|S(Ta_n,Ta_n,Tx)|\to 0.$$

Therefore $\{Ta_n\}$ is convergent to $Tx=x$. Consequently, T is continuous at x by Lemma 2.6. □

Remark 3.2. (1) Theorem 3.1 is a generalization of the Banach's contraction principle on complete complex valued S-metric spaces. Indeed, if we take $c_1=h$ and $c_2=c_3=c_4=0$ in Theorem 3.1, then we obtain the Banach's contraction condition in Theorem 2.7.

(2) If we take the function $S:X\times X\times X\to[0,\infty)$ in Theorem 3.1, Then we have Theorem 3 in [6].

Corollary 3.3. Let (X,S) be a complete complex valued S-metric space and T be a self-mapping of X. If there exist nonnegative real numbers c_1,c_2,c_3,c_4 satisfying $\max\{c_1+3c_3+2c_4,c_1+c_2+c_3,c_2+2c_4\}<1$ such that

$$\begin{aligned} S(T^px,T^px,T^py) &\preceq c_1S(x,x,y)+c_2S(T^px,T^px,y)+c_3S(T^py,T^py,x) \\ &\quad +c_4\max\{S(T^px,T^px,x),S(T^py,T^py,y)\}, \end{aligned}$$

for all $x,y\in X$ and some $p\in\mathbb{N}$, then T has a unique fixed point x in X and T^p is continuous at x.

Proof. Using the similar arguments in Theorem 3.1, we can easily see that T^p has a unique fixed point x in X and T^p is continuous at x. Also we obtain

$$Tx = TT^px = T^{p+1}x = T^pTx,$$

which implies that Tx is a fixed point of T^p. Consequently we have $Tx = x$ since x is a unique fixed point. □

Theorem 3.4. Let (X, S) be a complete complex valued S-metric space and T be a self-mapping of X. If there exist nonnegative real numbers $c_1, c_2, c_3, c_4, c_5, c_6$ satisfying $\max\{c_1 + c_2 + 3c_4 + c_5 + 3c_6, c_1 + c_3 + c_4 + c_6, 2c_2 + c_3 + 2c_6\} < 1$ such that

$$\begin{aligned} S(Tx, Tx, Ty) \preceq\ & c_1S(x, x, y) + c_2S(Tx, Tx, x) + c_3S(Tx, Tx, y) \\ & +c_4S(Ty, Ty, x) + c_5S(Ty, Ty, y) + c_6 \max\{S(x, x, y), \\ & S(Tx, Tx, x), S(Tx, Tx, y), S(Ty, Ty, x), S(Ty, Ty, y)\}, \end{aligned} \tag{8}$$

for all $x, y \in X$, then T has a unique fixed point x in X and T is continuous at x.

Proof. Let $a_0 \in X$ and the sequence $\{a_n\}$ be defined by

$$T^na_0 = a_n.$$

Assume that $a_n \neq a_{n+1}$ for all n. Using the inequality 8, the condition $(CS3)$ and Lemma 2.5, we obtain

$$\begin{aligned} S(a_n, a_n, a_{n+1}) &= S(Ta_{n-1}, Ta_{n-1}, Ta_n) \preceq c_1S(a_{n-1}, a_{n-1}, a_n) + c_2S(a_n, a_n, a_{n-1}) \\ &\quad +c_3S(a_n, a_n, a_n) + c_4S(a_{n+1}, a_{n+1}, a_{n-1}) + c_5S(a_{n+1}, a_{n+1}, a_n) \\ &\quad +c_6 \max\{S(a_{n-1}, a_{n-1}, a_n), S(a_n, a_n, a_{n-1}), S(a_n, a_n, a_n), \\ &\quad S(a_{n+1}, a_{n+1}, a_{n-1}), S(a_{n+1}, a_{n+1}, a_n)\} \\ &= c_1S(a_{n-1}, a_{n-1}, a_n) + c_2S(a_n, a_n, a_{n-1}) + c_4S(a_{n+1}, a_{n+1}, a_{n-1}) \\ &\quad +c_5S(a_{n+1}, a_{n+1}, a_n) + c_6 \max\{S(a_{n-1}, a_{n-1}, a_n), S(a_n, a_n, a_{n-1}), \\ &\quad S(a_{n+1}, a_{n+1}, a_{n-1}), S(a_{n+1}, a_{n+1}, a_n)\} \\ &\preceq (c_1 + c_2 + c_4 + c_6)S(a_{n-1}, a_{n-1}, a_n) \\ &\quad +(2c_4 + c_5 + 2c_6)S(a_{n+1}, a_{n+1}, a_n) \end{aligned}$$

and

$$S(a_n, a_n, a_{n+1}) \preceq \frac{c_1 + c_2 + c_4 + c_6}{2c_4 + c_5 + 2c_6}S(a_{n-1}, a_{n-1}, a_n). \tag{9}$$

Let $c = \frac{c_1+c_2+c_4+c_6}{2c_4+c_5+2c_6}$. Then we find $c < 1$ since $c_1 + c_2 + 3c_4 + c_5 + 3c_6 < 1$. Using the inequality (9), we obtain

$$S(a_n, a_n, a_{n+1}) \preceq c^nS(a_0, a_0, a_1). \tag{10}$$

For all $n, m \in \mathbb{N}$, $n < m$, using the inequality (10) and the condition $(CS3)$, we have

$$S(a_n, a_n, a_m) \preceq \frac{2c^n}{1 - c}S(a_0, a_0, a_1),$$

which implies

$$|S(a_n, a_n, a_m)| \preceq \frac{2c^n}{1-c} |S(a_0, a_0, a_1)| .$$

Therefore $|S(a_n, a_n, a_m)| \to 0$ as $n, m \to \infty$. Hence $\{a_n\}$ is a Cauchy sequence. Since (X, S) is complete, there exists $x \in X$ such that $\{a_n\}$ converges to x.

Now we show that x is a fixed point of T. Suppose that $Tx \neq x$. Then we get

$$\begin{aligned} S(a_n, a_n, Tx) &= S(Ta_{n-1}, Ta_{n-1}, Tx) \preceq c_1 S(a_{n-1}, a_{n-1}, x) + c_2 S(a_n, a_n, a_{n-1}) \\ &\quad + c_3 S(a_n, a_n, x) + c_4 S(Tx, Tx, a_{n-1}) + c_5 S(Tx, Tx, x) \\ &\quad + c_6 \max\{S(a_{n-1}, a_{n-1}, x), S(a_n, a_n, a_{n-1}), S(a_n, a_n, x), \\ &\quad S(Tx, Tx, a_{n-1}), S(Tx, Tx, x)\} \end{aligned}$$

and

$$\begin{aligned} |S(a_n, a_n, Tx)| &\leq c_1 |S(a_{n-1}, a_{n-1}, x)| + c_2 |S(a_n, a_n, a_{n-1})| + c_3 |S(a_n, a_n, x)| \\ &\quad + c_4 |S(Tx, Tx, a_{n-1})| + c_5 |S(Tx, Tx, x)| \\ &\quad + c_6 \left| \begin{array}{c} \max\{S(a_{n-1}, a_{n-1}, x), S(a_n, a_n, a_{n-1}), S(a_n, a_n, x), \\ S(Tx, Tx, a_{n-1}), S(Tx, Tx, x)\} \end{array} \right| . \end{aligned}$$

If we take limit for $n \to \infty$, then using the continuity of S and Lemma 2.5, we have

$$|S(Tx, Tx, x)| \leq (c_4 + c_5 + c_6) |S(Tx, Tx, x)| ,$$

which is a contradiction since $0 \leq c_4 + c_5 + c_6 < 1$. Hence we obtain $Tx = x$.

Now we show that x is unique. Let y be another fixed point of T such that $x \neq y$. Using the inequality (8) and Lemma 2.5, we have

$$\begin{aligned} S(Tx, Tx, Ty) &= S(x, x, y) \preceq c_1 S(x, x, y) + c_2 S(x, x, x) + c_3 S(x, x, y) \\ &\quad + c_4 S(y, y, x) + c_5 S(y, y, y) + c_6 \max\{S(x, x, y), \\ &\quad S(x, x, x), S(x, x, y), S(y, y, x), S(y, y, y)\} \end{aligned}$$

and

$$|S(x, x, y)| \leq (c_1 + c_3 + c_4 + c_6) |S(x, x, y)| ,$$

which implies $x = y$ since $c_1 + c_3 + c_4 + c_6 < 1$.

Now we prove that T is continuous at x. For $n \in \mathbb{N}$, using the inequality (8), the

condition $(CS3)$ and Lemma 2.5, we obtain

$$\begin{aligned} S(Ta_n, Ta_n, Tx) &\preceq c_1 S(a_n, a_n, x) + c_2 S(Ta_n, Ta_n, a_n) + c_3 S(Ta_n, Ta_n, x) \\ &\quad + c_4 S(Tx, Tx, a_n) + c_5 S(Tx, Tx, x) \\ &\quad + c_6 \max\{S(a_n, a_n, x), S(Ta_n, Ta_n, , a_n), S(Ta_n, Ta_n, x), \\ &\quad S(Tx, Tx, a_n), S(Tx, Tx, x)\} \\ &\preceq c_1 S(a_n, a_n, x) + 2c_2 S(Ta_n, Ta_n, x) + c_2 S(a_n, a_n, x) \\ &\quad + c_3 S(Ta_n, Ta_n, x) + c_4 S(Tx, Tx, a_n) \\ &\quad + c_6 \max\{S(a_n, a_n, x), 2S(Ta_n, Ta_n, x) + S(a_n, a_n, x), \\ &\quad S(Ta_n, Ta_n, x)\} \\ &= (c_1 + c_2 + c_4 + c_6) S(a_n, a_n, x) + (2c_2 + c_3 + 2c_6) S(Tx, Tx, Ta_n) \end{aligned}$$

and

$$(1 - 2c_2 - c_3 - 2c_6) S(Ta_n, Ta_n, Tx) \preceq (c_1 + c_2 + c_4 + c_6) S(a_n, a_n, x),$$

which implies

$$|S(Ta_n, Ta_n, Tx)| \leq \frac{c_1 + c_2 + c_4 + c_6}{1 - 2c_2 - c_3 - 2c_6} |S(a_n, a_n, x)|.$$

If we take limit for $n \to \infty$, then we have

$$|S(Ta_n, Ta_n, Tx)| \to 0.$$

Therefore $\{Ta_n\}$ is convergent to $Tx = x$. Consequently, T is continuous at x by Lemma 2.6. □

Remark 3.5. (1) Theorem 3.4 is a generalization of Banach's contraction principle on complete complex valued S-metric spaces. Indeed, if we take $c_1 = h$ and $c_2 = c_3 = c_4 = c_5 = c_6 = 0$ in Theorem 3.4, then we obtain the Banach's contraction condition in Theorem 2.7.

(2) If we take the function $S : X \times X \times X \to [0, \infty)$ in Theorem 3.4, Then we have Theorem 4 in [6].

Corollary 3.6. Let (X, S) be a complete complex valued S-metric space and T be a self-mapping of X. If there exist nonnegative real numbers $c_1, c_2, c_3, c_4, c_5, c_6$ satisfying $\max\{c_1 + c_2 + 3c_4 + c_5 + 3c_6, c_1 + c_3 + c_4 + c_6, 2c_2 + c_3 + 2c_6\} < 1$ such that

$$\begin{aligned} S(T^p x, T^p x, T^p y) &\preceq c_1 S(x, x, y) + c_2 S(T^p x, T^p x, x) + c_3 S(T^p x, T^p x, y) \\ &\quad + c_4 S(T^p y, T^p y, x) + c_5 S(T^p y, T^p y, y) + c_6 \max\{S(x, x, y), \\ &\quad S(T^p x, T^p x, x), S(T^p x, T^p x, y), S(T^p y, T^p y, x), S(T^p y, T^p y, y)\}, \end{aligned}$$

for all $x, y \in X$ and some $p \in \mathbb{N}$, then T has a unique fixed point x in X and T^p is continuous at x.

Proof. It follows from Theorem 3.4 by the same argument used in the proof of Corollary 3.3. □

In the following example we give a self-mapping satisfying the conditions of our results, but does not satisfy the condition of the Banach's contraction principle.

Example 3.7. Let $X = \mathbb{R}$ and the function $S : X \times X \times X \to \mathbb{C}$ be defined as

$$S(x, y, z) = e^{it}(|x - z| + |x + z - 2y|),$$

for all $x, y, z, t \in \mathbb{R}$. Then $(\mathbb{R}, S)$ is a complete complex valued S-metric space. Let us define the self-mapping $T : \mathbb{R} \to \mathbb{R}$ as follows:

$$Tx = \begin{cases} x + 70 & \text{if} \quad x \in \{0, 6\} \\ 65 & \text{if} \quad \text{otherwise} \end{cases},$$

for all $x \in \mathbb{R}$. Therefore T satisfies the inequality (2) in Theorem 3.1 for $c_1 = c_2 = c_3 = 0$, $c_4 = \frac{1}{4}$ and the inequality (8) in Theorem 3.4 for $c_1 = c_3 = c_4 = c_5 = 0$, $c_2 = c_6 = \frac{1}{5}$. So T has a unique fixed point $x = 65$. But T does not satisfy the Banach's contraction condition in Theorem 2.7. Indeed, for $x = 6$, $y = 2$, we obtain

$$S(Tx, Tx, Ty) = S(76, 76, 65) = 22e^{it} \preceq hS(x, x, y) = hS(6, 6, 2) = 8he^{it}$$

and

$$\left|22e^{it}\right| = 22 \leq \left|8he^{it}\right| = 8h,$$

which is a contradiction $h < 1$.

References

[1] A. Azam, M. Arshad and I. Beg, *Banach contraction principle on cone rectangular metric spaces*, Applicable Analysis and Discrete Mathematics 3 (2009) 236-241.

[2] S. U. Khan and A. Bano, *Common fixed point theorems for f-contraction mappings in TVS-valued cone metric space*, Journal of New Theory 2 (13) (2016) 96-103.

[3] N. M. Mlaiki, *Common Fixed Points in Complex S-Metric Space*, Advances in Fixed Point Theory 4 (4) (2014) 509-524.

[4] N. Y. Özgür and N. Taş, *Some fixed point theorems on S-metric spaces*, submitted for publication.

[5] N. Y. Özgür and N. Taş, *Some new contractive mappings on S-metric spaces and their relationships with the mapping* (**S25**), submitted for publication.

[6] N. Y. Özgür and N. Taş, *Some generalizations of fixed point theorems on S-metric spaces*, Essays in Mathematics and Its Applications in Honor of Vladimir Arnold, New York, Springer, 2016.

[7] N. Y. Özgür and N. Taş, *Common fixed points of continuous mappings on complex valued S-metric spaces*, submitted for publication.

[8] S. Sedghi, N. Shobe and A. Aliouche, *A generalization of fixed point theorems in S-metric spaces*, Matematicki Vesnik 64 (3) (2012) 258-266.

[9] S. Sedghi and N. V. Dung, *Fixed point theorems on S-metric spaces*, Matematicki Vesnik 66 (1) (2014) 113-124.

[10] S. Sedghi, İ. Altun, N. Shobe and M. A. Salahshour, *Some properties of S-metric spaces and fixed point results*, Kyungpook Mathematical Journal 54 (2014) 113-122.

http://www.newtheory.org **ISSN: 2149-1402**

Journal of New Theory

Received: 16.04.2016 *Year*: **2016,** *Number*: **14**, *Pages*: **37-45**
Published: 22.07.2016 *Original Article*[*]

INTERSECTIONAL SOFT SETS IN ORDERED GROUPOIDS

Essam Hamouda <ehamouda70@gmail.com>

Department of Basic Sciences, Faculty of Industrial Education, Beni-Suef University, Egypt

Abstract – In this note, the notions of soft int-ordered groupoids and soft left (resp., right) ideals are introduced. The characterization of int-soft ordered groupoids in terms of characteristic and inclusive sets is discussed. The concepts of soft prime ideals and soft int-filters are also introduced, and the relation between them is investigated.

Keywords *– Ordered groupoids, soft sets, int-soft filters, soft prime ideals.*

1. Introduction

The most successful theoretical approach to vagueness is undoubtedly fuzzy set theory introduced by Zadeh [14]. The theory is used commonly in different areas as engineering, medicine and economics, among others. The fuzzy set theory is based on the fuzzy membership function $\mu : X \to [0; 1]$. By the fuzzy membership function, we can determine the membership grade of an element with respect to a set. The fuzzy set theory has become very popular and has been used to solve problems in different areas. But there exists a difficulty: how to set the membership function in each particular case. The theory of soft sets is introduced by Molodtsov [8] as a new tool to discuss (vagueness) uncertainty. A soft set is a collection of approximate descriptions of an object. Each approximate description has two parts: a predicate and an approximate value set. In classical mathematics, we construct a mathematical model of an object and define the notion of the exact solution of this model. Usually the mathematical model is too complicated and we cannot find the exact solution. So, in the second step, we introduce the notion of approximate solution and calculate that solution. In the Soft Set Theory, we have the opposite approach to this problem. The initial description of the object has an approximate nature, and we do not need to introduce the notion of the exact solution. The absence of any restrictions on the approximate description in Soft Set Theory makes this theory very convenient and easily applicable in practice. Soft set theory has potential applications in many fields, including the smoothness of functions, game theory, operations research, Riemann integration, Perron integration, probability theory and measurement theory. Most

[*] *Edited by* Naim Çağman *(Editor-in-Chief).*

of these applications have already been demonstrated in Molodtsov's paper [8]. Authors in [13] gave an application of soft sets to diagnose the prostate cancer risk. Cagman et al. [2] applied the soft set to the theory of groups. They studied the soft int-groups, which are different from the definition of soft groups in [1, 9]. This new approach is based on the inclusion relation and intersection of sets. It brings the soft set theory, set theory and the group theory together. Some supplementary properties of soft int-groups and normal soft int-groups, analogues to classical group theory and fuzzy group theory are introduced in [3, 10]. Recently, Ideal theory in semigroups based on soft int-semigroup is investigated in [11]. Authors in [12] discussed the applications of fuzzy soft sets to ordered semi group theory. Khan et al. [7], presented the concepts of a fuzzy soft left (right) ideal and fuzzy soft interior ideal over an ordered semigroup.

In this paper, the notions of soft int-ordered groupoids and soft left (resp., right) ideals are introduced. The characterization of soft int-ordered groupoids in terms of characteristic and inclusive sets is discussed. The concepts of soft prime ideals and soft int-filters are also introduced, and the relation between them is investigated.

2. Preliminaries

We denote by $(S,.,\leq)$ an ordered groupiod, that is, a groupiod $(S,.)$ with a simple order $\leq$ which satisfies the following condition:

$$\forall\, x,y,z \in S,\ x \leq y \text{ implies } xz \leq yz \text{ and } zx \leq zy\,.$$

Definition 2.1. [5] A non-empty subset A of S is called a left (resp. right) ideal of S if
1) $SA \subseteq A$ (resp. $\subseteq A$)
2) $a \in A, S \ni b \leq a$ implies $b \in A$.

Definition 2.2. [5] A (non-empty) set *A* is called an ideal of *S* if it is both a left and a right ideal of *S*.

Definition 2.3. [4] A subgroupoid F of S is called a filter of S if
1) $a,b \in S, ab \in F$ implies $b \in F$,
2) $a \in F, S \ni b \geq a$ implies $a \in F$.

For $A \subseteq S$, we define $(A] = \{t \in S : t \leq a \text{ for some } a \in A\}$.

Let U be an initial universe set and let E be a set of parameters. Let $P(U)$ denote the power set of U and $A, B, C, \ldots \subseteq E$.

Definition 2.4. [8] A soft set (α, A) over U is defined to be the set of ordered pairs

$$(\alpha, A) = \{(x, \alpha(x)) : x \in E;\ \alpha(x) \in P(U)\}\,;$$

where $\alpha : E \to P(U)$ such that $\alpha(x) = \emptyset$ if $x \notin A$.

Definition 2.5. [11] Let (α, A) and (β, A) be two soft sets. Then, (α, A) is a soft subset of (β, A), denoted by $(\alpha, A) \sqsubseteq (\beta, A)$ if $\alpha(x) \subseteq \beta(x)$ for all $x \in A$ and (α, A); (β, A) are called soft equal, denoted by $(\alpha, A) = (\beta, A)$ if and only if $\alpha(x) = \beta(x)$ for all $x \in A$.

Definition 2.6. [11] Let (α, A) and (β, A) be two soft sets. Then, union $(\alpha, A) \sqcup (\beta, A)$ and intersection $(\alpha, A) \sqcap (\beta, A)$ are defined by

$$(\alpha \sqcup \beta)(x) = \alpha(x) \cup \beta(x),$$
$$(\alpha \sqcap \beta)(x) = \alpha(x) \cap \beta(x),$$

respectively.

Definition 2.7. A soft set (α, S) in a groupoid S is called a soft int- subgroupoid of S if

$$\alpha(xy) \supseteq \alpha(x) \cap \alpha(y) \text{ for all } x, y \in S.$$

3. Soft Left and Soft Right Ideals in Ordered Groupoids

In what follows, we take $E = S$, as a set of parameters , which is a groupoid unless otherwise stated. For a nonempty subset A of S, define a map $\chi_A : S \to P(U)$ as follows:

$$\chi_A(x) = \begin{cases} U & \text{if } x \in A, \\ \emptyset & \text{otherwise.} \end{cases}$$

Then (χ_A, S) is a soft set over U, which is called the characteristic soft set (see [11]).

Lemma 3.1. If $(S, ., \leq)$ is an ordered groupoid and $\emptyset \neq A \subseteq S$, the characteristic Soft set $(\chi_{(A]}, S)$ is satisfying the condition:

$$\forall x, y \in S, x \leq y \text{ implies } \chi_{(A]}(x) \supseteq \chi_{(A]}(y).$$

Proof. By definition, $\chi_{(A]}$ is a mapping from S into $\{U, \emptyset\} \subset P(U)$. Suppose $x, y \in S$, $x \leq y$ .If $y \notin (A]$, then $\chi_{(A]}(y) = \emptyset$ and $\chi_{(A]}(x) \supseteq \chi_{(A]}(y)$. Consider the case $y \in (A]$, then $\chi_{(A]}(y) = U$. Because $y \in (A]$, there exists $z \in A$ such that $y \leq z$ and consequently $x \leq z$. Thus $x \in (A]$. Therefore, $\chi_{(A]}(x) = U$, $\chi_{(A]}(x) \supseteq \chi_{(A]}(y)$. ■

Proposition 3.2. Let $(S, ., \leq)$ be an ordered groupoid and $\emptyset \neq A \subseteq S$. Then $A = (A]$ if and only if (χ_A, S) satifies

$$\forall x, y \in S, x \leq y \text{ implies } \chi_A(x) \supseteq \chi_A(y).$$

Proof. Assume that $A = (A]$, the desired result comes directly from lemma 3.1. Conversely, suppose that for $x, y \in S$, $x \leq y$ implies $\chi_A(x) \supseteq \chi_A(y)$. Let $x \in (A]$. There exists $y \in A$ so that $x \leq y$. By the hypothesis, we have $\chi_A(x) \supseteq \chi_A(y)$. Since $y \in A$, we have $\chi_A(y) = U$. Thus $\chi_A(x) = U$ and $x \in A$. Therefore $A = (A]$. ■

Here, we introduce the concepts of soft (left, right) ideals in ordered groupoids and characterize them in terms of soft sets.

Definition 3.3. Let $(S, ., \leq)$ be an ordered groupoid. A soft set (α, S) over U is called a soft left ideal over U if

1) $\alpha(xy) \supseteq \alpha(y)$ for all $x, y \in S$,
2) $x \leq y$ implies $\alpha(x) \supseteq \alpha(y)$.

Definition 3.4. Let $(S, ., \leq)$ be an ordered groupoid. A soft set (α, S) over U is called a soft right ideal over U if

1) $\alpha(xy) \supseteq \alpha(x)$ for all $x, y \in S$,
2) $x \leq y$ implies $\alpha(x) \supseteq \alpha(y)$.

A soft set (α, S) over U is called a soft ideal over U if it is both a soft left and a soft right ideal over U.

Theorem 3.5.[11**]** For any nonempty subset A of a groupoid S, the following are equivalent.

1) A is a left (resp., right) ideal of S.
2) The characteristic soft set (χ_A, S) is a soft left (resp., right) ideal over U.

Theorem 3.6. Let $(S, ., \leq)$ be an ordered groupoid, and $\emptyset \neq A \subseteq S$. Then A is a left (right) ideal of S if and only if (χ_A, S) is a soft left (right) ideal over U .

Proof. Assume that A is a left ideal of S. For any $x, y \in S$, $x \leq y$. If $y \notin A$ then $\chi_A(y) = \emptyset$ and $\chi_A(x) \supseteq \chi_A(y)$. It is clear that $\chi_A(xy) \supseteq \emptyset = \chi_A(y)$. If $y \in A$, then $x.y \in A$ and $\chi_A(y) = U$. Since $x \leq y$ and A a left ideal of S, we have $y \in A$ and so $\chi_A(x) = U$. Thus again $\chi_A(x) \geq \chi_A(y)$ and $\chi_A(xy) = U = \chi_A(y)$. Therefore, (χ_A, S) is a soft left ideal over U. Similarly, (χ_A, S) is a soft right ideal over U when A is a left ideal of S. Conversely, suppose that (χ_A, S) is a soft left ideal over U. Let $x \in S$ and $y \in A$ such that $x \leq y$. Then $\chi_A(y) = U$, and so $\chi_A(xy) \supseteq \chi_A(y) = U$. Since (χ_A, S) is a soft left ideal over U and $\leq y$, we have $\chi_A(x) \supseteq \chi_A(y)$. Since $y \in A$, $\chi_A(y) = U$. Then $\chi_A(x) = U$, and $x \in A$. The rest of the proof is a consequence of theorem 3.5. Similarly, we can show that if (χ_A, S) is a soft right ideal over U, then A is a right ideal of S. ■

Definition 3.7.[10] For a soft set (α, A) over U and a non-empty subset V of U, the V-inclusive set of (α, A), denoted by α^V, is defined to be the set

$$\alpha^V = \{x \in A : V \subseteq \alpha(x)\}.$$

As a generalization of Theorem 3.6, we have the following result.

Theorem 3.8. Let $(S, \cdot, \leq)$ be an ordered groupoid and (α, S) a soft set over U. Then (α, S) is a soft ideal over U if and only if α^V is an ideal of S provided $\alpha^V = \emptyset$.

Proof. Assume that (α, S) is a soft ideal over U. Let $x \in \alpha^V$, then $\alpha(x) \supseteq V$. Since (α, S) is a soft ideal, we have $\alpha(xy) \supseteq \alpha(x) \supseteq V$ and $\alpha(yx) \supseteq \alpha(x) \supseteq V$ for all $y \in S$. Thus $xy \in \alpha^V$ and $yx \in \alpha^V$. Furthermore, let $x \in \alpha^V$ and $y \in S$ such that $y \leq x$. Then $y \in \alpha^V$. Indeed, since $x \in \alpha^V$, $\alpha(x) \supseteq V$, and (α, S) is a soft ideal over U, we have $\alpha(y) \supseteq \alpha(x) \supseteq V$, so $y \in \alpha^V$. Therefore, α^V is an ideal of S. Conversely, let α^V be an ideal of S for every non-empty subset $V \subseteq U$. For any $\in S$, take $V = \alpha(x)$. Then $x \in \alpha^V$. Since α^V is an ideal of S, we have $xy \in \alpha^V$ and so $\alpha(xy) \supseteq V = \alpha(x)$, for all $y \in S$.

Moreover, if $x \leq y$ then $\alpha(x) \supseteq \alpha(y)$. Indeed: Let $\alpha(y) = W$. Then $y \in \alpha^W$. Since $\alpha^W$is an ideal of S, we have $x \in \alpha^W$. Then $(x) \supseteq W = \alpha(y)$. Therefore, (α, S) is a soft right ideal over U. In a similar way, we can show that (α, S) is also a soft left ideal over U, and so (α, S) is a soft ideal over U. ■

For an ordered groupoid S, let (θ, S) be the soft set over U defined by $\theta(x) = U$ for all $x \in S$. Let $a \in S$, define $A_a = \{(x,y) \in S \times S : a \leq xy\}$. For two soft sets (α, S) and (β, S) , we define The soft product of (α, S) and (β, S) as the soft set $(\alpha \circ \beta, S)$ over U defined by

$$(\alpha o \beta)(a) = \begin{cases} \bigcup_{(x,y)\in A_a} \{\alpha(x) \cap \beta(y)\} & if\ A_a \neq \emptyset \\ \emptyset & otherwise \end{cases}$$

Here, we give equivalent definitions of soft right (resp. left) ideals and soft ideals.

Theorem 3.9.. Let $(S, ., \leq)$ be an ordered groupoid. A soft set (α, S) over U is called a soft left ideal over U if and only if

1) $(\theta \circ \alpha, S) \sqsubseteq (\alpha, S)$,
2) $x \leq y$ implies $\alpha(x) \supseteq \alpha(y)$.

Proof. Assume that (α, S) is a soft left ideal over U. Let $a \in S$. Then $(\theta \circ \alpha)(a) \subseteq \alpha(a)$. Indeed: If $A_a = \emptyset$, then $(\theta \circ \alpha)(a) = \emptyset \subseteq \alpha(a)$. Let $A_a \neq \emptyset$. Then

$$(\theta \circ \alpha)(a) = \bigcup_{(x,y)\in A_a} \{\theta(x) \cap \alpha(y)\}$$

$$= \bigcup_{(x,y)\in A_a} \{\alpha(y)\}$$

Now, we show that $\alpha(y)) \subseteq \alpha(a)$ for every $(x, y) \in A_a$. In fact: If $(x, y) \in A_a$, then $a \leq xy$. Since (α, S) is a soft left ideal, we have $\alpha(a) \supseteq \alpha(xy) \supseteq \alpha(y)$. Therefore we have

$$(\theta \circ \alpha)(a) = \bigcup_{(x,y)\in A_a} \{\theta(x) \cap \alpha(y)\}$$

$$= \bigcup_{(x,y)\in A_a} \{\alpha(y)\} \subseteq \alpha(a)$$

Conversely, let $x, y \in S$. By hypothesis, we have $(\theta \circ \alpha)(xy) \subseteq \alpha(xy)$. Since $(x, y) \in A_{xy}$, we have

$$(\theta \circ \alpha)(xy) = \bigcup_{(s,t)\in A_{xy}} \{\theta(s) \cap \alpha(t)\}$$

$$\supseteq \theta(x) \cap \alpha(y) = \alpha(y)$$

Hence we obtain $\alpha(xy) \supseteq \alpha(y)$, that is, (α, S) is a soft left ideal over U . ■

In a similar argument we prove the following result**.**

Theorem 3.10. Let $(S,.,\leq)$ be an ordered groupoid. A soft set (α,S) over U is called a soft ideal ideal over U if and only if

1) $(\alpha\circ\theta,S)\sqsubseteq(\alpha,S)$,
2) $x\leq y$ implies $\alpha(x)\supseteq\alpha(y)$.

Theorem 3.11. Let $(S,.,\leq)$ be an ordered semigroup. S is regular if and only if for every soft set (α,S) over U we have $(\alpha,S)\sqsubseteq(\alpha\circ\theta\circ\alpha,S)$.

Proof. Assume that S is regular and that (α,S) is a soft set over U. For $a\in S$ there exists $x\in S$ such that $a\leq axa$. Since $(ax,a)\in A_a$, we have

$$(\alpha\circ\theta\circ\alpha)(a)=\bigcup_{(s,t)\in A_a}\{(\alpha\circ\theta)(s)\cap\alpha(t)\}$$

$$\supseteq(\alpha\circ\theta)(ax)\cap\alpha(a).$$

Since $(a,x)\in A_{ax}$, we have

$$(\alpha\circ\theta)(ax)=\bigcup_{(u,v)\in A_{ax}}\{(\alpha)(u)\cap\theta(v)\}$$

$$\supseteq\alpha(a)\cap\theta(x)=\alpha(a).$$

Hence we have $(\alpha\circ\theta\circ\alpha)(a)\supseteq\alpha(a)$. Therefore, $(\alpha,S)\sqsubseteq(\alpha\circ\theta\circ\alpha,S)$. Conversely, Let $a\in S$. By hypothesis, we have

$$\chi_{\{a\}}(a)=U\subseteq(\chi_{\{a\}}\circ\theta\circ\chi_{\{a\}})(a).$$

Thus

$$(\chi_{\{a\}}\circ\theta\circ\chi_{\{a\}})(a)=U.$$

If $A_a=\emptyset$, then $(\chi_{\{a\}}\circ\theta\circ\chi_{\{a\}})(a)=\emptyset$, a contradiction. So $A_a\neq\emptyset$, then

$$(\chi_{\{a\}}\circ\theta\circ\chi_{\{a\}})(a)=$$
$$\cup_{(x,y)\in A_a}\{(\chi_{\{a\}}\circ\theta)(x)\cap\chi_{\{a\}}(y)\}.$$

Claim: There exists $(x,y)\in A_a$ such that $(\chi_{\{a\}}\circ\theta)(x)\neq\emptyset$ and $\chi_{\{a\}}(y)\neq\emptyset$.
Proof. Suppose that $(\chi_{\{a\}}\circ\theta)(x)=\emptyset$ or $\chi_{\{a\}}(y)=\emptyset$ for every $(x,y)\in A_a$, then $(\chi_{\{a\}}\circ\theta)(x)\cap\chi_{\{a\}}(y)=\emptyset$ for every $(x,y)\in A_a$. This implies that

$$(\chi_{\{a\}}\circ\theta\circ\chi_{\{a\}})(a)=\bigcup_{(x,y)\in A_a}\{(\chi_{\{a\}}\circ\theta)(u)\cap\chi_{\{a\}}(v)\}=\emptyset.$$

But this contradicts

$$(\chi_{\{a\}}\circ\theta\circ\chi_{\{a\}})(a)=U.$$

If $y \neq a$, then $\chi_{\{a\}}(y) = \emptyset$. By the claim, we have $y = a$, $(x, a) \in A_a$ and $a \leq xa$. Let A_a be empty, then $(\chi_{\{a\}} \circ \theta)(x) = \emptyset$. By the claim, we have $A_a \neq \emptyset$. Then

$$(\chi_{\{a\}} \circ \theta)(x) = \bigcup_{(s,t)\in A_x} \{\chi_{\{a\}}(s) \cap \theta(t)\} = \bigcup_{(s,t)\in A_x} \{\chi_{\{a\}}(s)\}$$

If $s \neq a$ for every $(s, t) \in A_x$, then $\chi_{\{a\}}(s) = \emptyset$. Hence $(\chi_{\{a\}} \circ \theta)(x) = \emptyset$. By the claim, there exists $(s, t) \in A_x$ such that $s = a$. Then $(a, t) \in A_x$ and $x \leq at$. Thus we have $a \leq xa \leq ata$. Therefore, S is regular. ■

4. Soft Filters in Ordered Groupoids

In this section, we introduce the concept of int-soft filters in ordered groupoids, and we characterize filters of ordered groupoids in terms of int-soft filters.

Definition 4.1. Let $(S, \cdot, \leq)$ be an ordered groupoid. A soft set (α, S) over U is called a soft int-filter over U if

1) $x \leq y \Rightarrow \alpha(x) \leq \alpha(y)$.
2) $\alpha(xy) = \alpha(x) \cap \alpha(y)\ \forall\ x, y \in S$.

It is well known that a subset A of a groupoid S is a subgroupoid iff the soft set (χ_A, S) is a soft int-groupoid over U [11].

Proposition 4.2. Let $(S, \cdot, \leq)$ be an ordered groupoid and $\emptyset \neq F \subseteq S$. Then F is a filter of S if and only if the soft set (χ_F, S) is a soft int-filter over U.

Proof. Assume that F is a filter of S and that $x, y \in S, x \leq y$. If $x \notin F$, then $\chi_F(x) = \emptyset$. Hence $\chi_F(x) \subseteq \chi_F(y)$. If $x \in F$, then $\chi_F(x) = U$. Since $y \geq x \in F$, we have $y \in F$. Then $\chi_F(y) = U$, and again $\chi_F(x) \subseteq \chi_F(y)$. In order to show that $\chi_F(xy) = \chi_F(x) \cap \chi_F(y)$ for all $x, y \in S$, let $x, y \in S$ such that $x.y \notin F$. Then $\chi_F(xy) = \emptyset$. Moreover $x.y \notin F$ implies $x \notin F$ or $y \notin F$. Then $\chi_F(x) = \emptyset$. or $\chi_F(y) = \emptyset$. So $\chi_F(x) \cap \chi_F(y) = \emptyset$, and $\chi_F(xy) = \chi_F(x) \cap \chi_F(y)$ for all $x, y \in S$. Now, consider $x.y \in F$. Then $\chi_F(xy) = U$. Since $x.y \in F$, we have $x \in F$ and $y \in F$. Then $\chi_F(x) = \chi_F(y) = U$, whence $\chi_F(x) \cap \chi_F(y) = U$ and $\chi_F(xy) = U = \chi_F(x) \cap \chi_F(y)$. Conversely, let (χ_F, S) be a soft int-filter over U. By the condition 2 of definition 4.1, F is a sub-groupoid of S. Let $x, y \in S$, $xy \in F$. Since (χ_F, S) is a soft int-filter over U, then $\chi_F(xy) = \chi_F(x) \cap \chi_F(y)$. Since $y \in F$, we have $\chi_F(xy) = U$. Then $\chi_F(x) \cap \chi_F(y) = U$, $\chi_F(x) = \chi_F(y) = U$, and $x, y \in F$. Let $x \in F$, $x \leq y$. Then we have $\chi_F(x) = U$. Since $x \leq y$, we have $\chi_F(x) \leq \chi_F(y)$. Therefore, $\chi_F(y) = U$, and $y \in F$. This completes the proof. ■

In the rest of this section, we give the relation between int-soft filters and soft prime ideals of ordered groupoids. In an ordered groupoid, a non-empty subset F is a filter if and only if $S \setminus F = \emptyset$ or $S \setminus F$ is a prime ideal of S [6]. An analogous result holds for soft sets, as well.

Definition 4.3. Let S be an ordered groupoid and (α, S) a soft set over . The complement of (α, S) is the soft set (α^c, S) defined by

$$\alpha^c : S \to P(U)$$

where $\alpha^c(x) = U \setminus \alpha(x)$.

Lemma 4.4. Let S be a groupoid and (α, S) a soft set over U. The following are equivalent:
1) $\alpha(xy) = \alpha(x) \cap \alpha(y), \forall x, y \in S$,
2) $\alpha^c(xy) = \alpha^c(x) \cup \alpha^c(y) \; \forall \; x, y \in S$.

Proof. Straightforward. ■

Definition 4.5. For a groupoid S, a soft set (α, S) over U is called a soft prime ideal over U if

$$\alpha(xy) \subseteq \alpha(x) \cup \alpha(y), \forall x, y \in S .$$

Theorem 4.6. Let $(S, \cdot, \leq)$ be an ordered groupoid and (α, S) a soft set over U. Then (α, S) is a soft int-filter over U if and only if (α^c, S) is an soft prime ideal over U .

Proof. Suppose (α, S) is a soft int-filter over U. Let $x, y \in S$, $x \leq y$. Then, we have$\alpha(x) \subseteq \alpha(y)$. Then $\alpha^c(x) = U \setminus \alpha(x) \supseteq U \setminus \alpha(y) = \alpha^c(y)$. Now, for any $x, y \in S$, we have $\alpha(xy) = \alpha(x) \cap \alpha(y)$. Then by lemma 4.4, $\alpha^c(xy) = \alpha^c(x) \cup \alpha^c(x)$. Therefore, (α^c, S) is an soft prime ideal over U. Conversely, Let $x, y \in S$, $x \leq y$. Since(α^c, S) is a soft ideal, we have $\alpha^c(x) \supseteq \alpha^c(y)$, and consequently $\alpha(x) \subseteq \alpha(y)$. Since$(\alpha^c, S)$ is an soft prime ideal, we have $\alpha^c(xy) = \alpha^c(x) \cup \alpha^c(x). \forall x, y \in S$. Then, by lemma 4.4, $\alpha(xy) = \alpha(x) \cap \alpha(y)$. Therefore, (α, S) is a soft int-filter over U. ■

References

[1] H. Aktas, N. Cagman, *Soft sets and soft groups*, Inform. Sci. 177 (2007) 2726-2735.

[2] N. Cagman, F. C. Tak, H. Aktas, *Soft int-group and its applications to group theory*, Neural. Comput. Appl. 21(2012) 151-158.

[3] K. Kaygsz, *On soft int-groups*, Ann. Fuzzy Math. Inform. 4 (2) (2012). 365-375.

[4] N. Kehayopulu, *On weakly commutative poe-semigroups*, Semigroup Forum 34 (1987) 367– 370.

[5] N. Kehayopulu, *On weakly prime ideals of ordered semigroups*, Math. Japonica 35(1990) 1051–1056.

[6] N. Kehayopulu, M. Tsingelis, *Fuzzy sets in ordered groupoids*, Semigroup Forum 65(2002) 128 – 132.

[7] A. Khan, N. Sarmin, F. Khan, B. Davvaz, *A study of fuzzy soft interior ideals of ordered semigroups*, Iranian Journal of Science & Technology, 37A3: (2013) 237-249

[8] D. A. Molodtsov, *Soft set theory first results*, Computers and Mathematics with Applications 37 (1999) 19-31.

[9] A. Sezgin, A. Atagun, *Soft groups and normalistic soft groups*, Computers and Mathematics with Applications 62(2) (2011) 685-698.

[10] I. Simsek, N. Cagman, K. Kaygisiz, *On normal soft intersection groups*, Contemp. Analy. And Appl. Math.,Vol.2, No.2 (2014) 258-267.

[11] S. Song, H. Kim, Y. Jun, *Ideal theory in semigroups based on intersectional soft sets*, The Scientific World J. Vol.2014, Article ID136424, (2014) 7 pages.
[12] G. Sun, Y. Li, Y. Yin Y, *New characterizations of regular ordered semigroups in terms of fuzzy soft ideals*, Mathematica Aeterna, Vol. 3, , no.7 (2013) 545 – 554
[13] S. Yuksela, T. Dizman, G. Yildizdan, U. Sertc, *Application of soft sets to diagnose the prostate cancer Risk*, Journal of Inequalities and Applications 2013, 2013:229
[14] L. A. Zadeh, *Fuzzy sets*, Inf. Control 8 (1965) 338-353.

http://www.newtheory.org **ISSN: 2149-1402**

Journal of New Theory

Received: 20.04.2015 *Year*: **2016**, *Number*: **14**, *Pages*: **46-57**
Published: 22.07.2016 *Original Article*[**]

FRAGMENTED CAESAR CIPHER

Yunus Aydoğan <yunus.programmer@gmail.com>
Naim Çağman <naim.cagman@gop.edu.tr>
Irfan Şimşek[*] <irfan.simsek@gop.edu.tr>

Department of Mathematics, Faculty of Arts and Sciences, Gaziosmanpaşa University
60240 Tokat, Turkey

Abstract — In this study, we define a cipher method that is called fragmented Caesar cipher method that based on the basic logic of Caesar cipher. This new method has more possibility then the classical Caesar cipher because of the fragmented alphabet is used to cipher. We then construct a mathematical modeling and make a computer programs of the method.

Keywords — *Caesar cipher, encryption, decryption, plaintext, ciphertext, fragmented Caesar cipher.*

1 Introduction

One of the earliest known cryptographic systems was used by Julius Caesar. In the Caesar cipher, each letter in a plaintext is shifted by a letter a certain number of positions down the alphabet. The Caesar cipher can be decrypted an easy way with the brute-force attack. Since then a lots of technics of cipher have been developed to obtain an unbroken cipher technic. For examples, Omolara *et al.* [5], Patni [7, 8], Dey *et al.* [2] and Mishra [4]. More detailed explanations related to the Caesar cipher can be found in [9] and [6].

In this study, we define a cipher method that is called fragmented Caesar cipher method that is based on the Caesar cipher. In the fragmented Caesar cipher, the alphabet broken into small fragments and each letter in each fragment is replaced by a letter some arbitrary number of positions down. We then construct a mathematical

[**] *Edited by* Oktay Muhtaroğlu *(Area Editor)*
[*] *Corresponding Author.*

modeling and make a computer programs of the method. We finally give an example to show the cipher method is working successfully.

The present paper is a condensation of part of the dissertation [1].

2 Fragmented Caesar Cipher Method

In this section, we define a new cipher method which depends on the Caesar cipher method. In this method, we firstly divide the alphabet arbitrary fragments. And then each letter in each fragment is replaced by a letter some fixed number of positions down. Therefor, we call this method as fragmented Caesar cipher method or in sort FCC-method.

2.1 Mathematical Model of FCC-method

In this subsection, we first give a mathematical model of the FCC-method. We then write an algorithm of the FCC-method to make a computer program.

Throughout this paper, ASCII (**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange) is used, $I_n = \{1, 2, ..., n\}$ for all $n \in \mathbb{N}$ is an index set and U is a set of using characters which is ordered according to the ASCII.

Definition 1. Let $|U| = n$ and $X = \{x_i : i \in I_n\}$ be an ordered set according to the index set I_n. Then,

$$\alpha : U \to X, \quad \alpha(i\text{-th element}) = x_i, i \in I_n,$$

is called **indexing function** of U. Here, x_i is called **indexed element** of ith element of U and the set X is called **indexed character set** of U.

Example 2. Let 1, 9, b, M, $<$ and $+$ be using characters. Then, the character set U is written as $U = \{+, 1, 9, <, M, b\}$ since

x	$+$	1	9	$<$	M	b
$ASCII$	43	49	57	60	77	98

Therefore the indexed character set of U is obtained as $X = \{x_1, x_2, x_3, x_4, x_5, x_6\}$ since

x	$+$	1	9	$<$	M	b
$\alpha(x)$	x_1	x_2	x_3	x_4	x_5	x_6

Definition 3. Let X be an indexed character set and $|X| = n$. Then, for $a_p \in \mathbb{N}$, $p \in I_n$, a fragmentation algorithm is set up as follows:

Algorithm of Fragmentation:

Step 1: Choose a_1 such that $2 \leq a_1 \leq n_1 = n - 2$

Step 2: Let $n_2 = n_1 - a_1$. If $n_2 > 4$, choose a_2 such that $2 \leq a_2 \leq n_2 - 2$, if not $a_2 = n_2$ which means the process is terminated.

$\vdots$

Step p: Let $n_p = n_{p-1} - a_{p-1}$. If $n_p > 4$, choose a_p such that $2 \leq a_p \leq n_p - 2$, if not $a_p = n_p$ which means the process is terminated.

Here, p is called a **fragment number**, a_p is number of characters in a fragment and $P = (a_1, a_2, ..., a_p)$ is called **fragment key** of X.

We can briefly choose values a_p as follow, for $p \in I_n$ and $i \in I_p$,

$$\begin{cases} 2 \leq a_1 \leq n_1, & \text{if } p = 1,\ n_1 = n - 2 \\ 2 \leq a_p \leq n_i - 2, & \text{if } p > 1,\ 4 < n_p,\ n_p = n_{p-1} - a_{p-1} \\ n_p = a_p, & \text{if } p > 1,\ n_p < 4,\ n_p = n_{p-1} - a_{p-1} \end{cases}$$

Example 4. Let X be an indexed character set and $|X| = 13$. If the fragmentation algorithm is working as follows,

Step 1: Choose $a_1 = 5$ such that $2 \leq a_1 \leq n_1 = 13 - 2 = 11$,

Step 2: Choose $a_2 = 6$ such that $2 \leq a_2 \leq 8 - 2$, because of $n_2 = 13 - 5 = 8$ and $8 > 4$,

Step 3: Choose $a_3 = 2$ because of $n_3 = 8 - 6 = 2$ and $2 < 4$.

Then, we obtain that $p = 3$ and $P = (5, 6, 2)$.

Definition 5. Let $X = \{x_1, x_2, ..., x_n\}$ be an indexed character set. For all $i \in I_n$ and $k \in I_{n-i}$, the set $W = \{x_i, x_{i+1}, ..., x_{i+k}\}$ is called as a **block subset** of X and denoted by $W \sqsubseteq X$.

Definition 6. Let X be an indexed character set, p be a number of fragment of X. If $X_i \sqsubseteq X$ has the following conditions, then family of set $\{X_i : i \in I_p\}$ is called an **ordered fragmentation** of X.

1. $|X_i| = a_i$,
2. $X_i \cap X_j = \emptyset$ for $i, j \in I_p$, $i \neq j$,
3. $X = \bigcup_{i \in I_p} X_i$,
4. $x_{max(X_i)+1} = x_{min(X_{i+1})}$ for $i \in I_p$, where $x_{min(X_i)}$ and $x_{max(X_i)}$ be the first and the last element of X_i, respectively.

Here, the X_i is called a **fragment** of X for $i \in I_p$.

Example 7. Let us consider Example 4 where $X = \{x_1, x_2, ..., x_{13}\}$ and $P = (5, 6, 2)$. Then, for $a_1 = 5$, $a_2 = 6$ and $a_3 = 2$ the ordered fragmentation of X are respectively as follow,

$$\begin{aligned} X_1 &= \{x_1, x_2, x_3, x_4, x_5\} \\ X_2 &= \{x_6, x_7, x_8, x_9, x_{10}, x_{11}\} \\ X_3 &= \{x_{12}, x_{13}\} \end{aligned}$$

Therefor, the ordered fragmentation of X is obtained as $\{X_1, X_2, X_3\}$.

Definition 8. Let X_i be a fragment of X and a_i be the number of X_i for all $i \in I_p$. If $0 < r_i < a_i$, then $R = (r_1, r_2, ..., r_p)$ is called **rotation key** of X.

Here, the r_i is called a **number of rotation** of X_i for all $i \in I_p$.

Note that the key of this method has two part, one of them is a fragment key P and the other is a rotation key R.

Example 9. Let us consider Example 4, if we choose number of rotations $r_1 = 3$, $r_2 = 4$ and $r_3 = 1$ for X_1, X_2, X_3, respectively. Then, the rotation key of X would be $R = (3, 4, 1)$.

Definition 10. Let X be an indexed character set, $\{X_1, X_2, ..., X_p\}$ be an ordered fragmentation of X and $P = (a_1, a_2, ..., a_p)$ be a fragment key of X. Then, m_i is defined by

$$m_i = \begin{cases} 0, & i = 0 \\ m_{i-1} + a_i, & i \in I_p \end{cases}$$

and called a **module** of X_i for all $i \in I_p$.

It is clear to see that $x_{m_i} = x_{max(X_i)}$ for $i \in I_p$.

Definition 11. Let X be an indexed character set and $\{X_1, X_2, ..., X_p\}$ be an ordered fragmentation of X. If m_i is a module of X_i for all $i \in I_p$ and $R = (r_1, r_2, ..., r_p)$ is a rotation key of X, then X_i**-rotation function**, denoted by β_i, is defined by

$$\beta_i : X_i \to X_i,\ \beta_i(x_t) = \begin{cases} x_{t+r_i}, & t + r_i \leq m_i \\ x_{(t+r_i)(mod\, m_i)+m_{i-1}}, & t + r_i > m_i \end{cases}$$

where $t \in I_{a_i}$.

Definition 12. Let X be an indexed character set and $\{X_1, X_2, ..., X_p\}$ be an ordered fragmentation of X. If β_i is an X_i-rotation function for all $i \in I_p$, then the following function

$$\beta : X \to X,\ \beta(x) = \begin{cases} \beta_1(x), & x \in X_1 \\ \beta_2(x), & x \in X_2 \\ \quad \vdots & \\ \beta_p(x), & x \in X_p \end{cases}$$

is called a **rotation function** of X.

Definition 13. Let $\alpha : U \to X$ be an indexing function. Then for all $t \in I_n$, inverse of α is called a **characterization function** and defined by

$$\alpha^{-1} : X \to U, \quad \alpha^{-1}(x_t) = \text{"}t\text{-th element of U "}$$

Definition 14. If $\alpha : U \to X$, $\alpha^{-1} : X \to U$ and $\beta : X \to X$ be indexing, characterization and rotation functions, respectively, then an **encryption function** on U is defined by

$$\gamma : U \to U, \quad \gamma(x) = \alpha^{-1}(\beta(\alpha(x)))$$

Definition 15. Let X be an indexed character set and $\{X_1, X_2, ..., X_p\}$ be an ordered fragmentation of X. If $R = (r_1, r_2, ..., r_p)$ is a rotation key of X, $\beta_i : X_i \to X_i$ is an X_i-rotation function and m_i is a module of X_i for all $i \in I_p$, then **inverse of rotation function** of X_i, denoted by β_i^{-1}, is defined by

$$\beta_i^{-1} : X_i \to X_i,$$
$$\beta_i^{-1}(x_t) = \begin{cases} x_{t+m_i-(r_i+m_{i-1})}, & t+m_i-(r_i+m_{i-1}) \leq m_i \\ x_{(t+m_i-(r_i+m_{i-1}))(mod\, m_i)+m_{i-1}}, & t+m_i-(r_i+m_{i-1}) > m_i \end{cases} \text{ where } t \in I_{a_i}.$$

Definition 16. Let X be an indexed character set and $\{X_1, X_2, ..., X_p\}$ be an ordered fragmentation of X. If β_i^{-1} is an inverse of rotation function of X_i for all $i \in I_p$, then the following function

$$\beta^{-1} : X \to X,\ \beta^{-1}(x) = \begin{cases} \beta_1^{-1}(x), & x \in X_1 \\ \beta_2^{-1}(x), & x \in X_2 \\ \quad \vdots & \\ \beta_p^{-1}(x), & x \in X_p \end{cases}$$

is called a **inverse of rotation function** of X.

Definition 17. If $\alpha : U \to X$, $\alpha^{-1} : X \to U$, $\beta^{-1} : X \to X$ and $\gamma : U \to U$ be indexing, characterization, inverse of rotation and encryption functions, respectively, then a **decryption function** on U is defined by

$$\gamma^{-1} : U \to U, \quad \gamma^{-1}(x) = \alpha^{-1}(\beta^{-1}(\alpha(x)))$$

It is clear to see that $\gamma^{-1}(x) = \alpha^{-1}(\beta^{-1}((\alpha^{-1})^{-1}(x))) = \alpha^{-1}(\beta^{-1}(\alpha(x)))$.

Definition 18. Let U be a character set, P be a fragment key, R be a rotation key and γ be an encryption function. The four tuple (U, P, R, γ) is called an **FCC-encryption** on U. The four tuple (U, P, R, γ^{-1}) is called an **FCC- decryption** on U.

2.2 FCC-Encryption Algorithm

Assume that U is a character set and X is an indexed character set. Then, an algorithm of the FCC-encryption is set up as follows:

Algorithm of FCC-Encryption:

Step 1: Find the fragment number p and the $P = (a_1, a_2, ..., a_p)$,
Step 2: Choose the $R = (r_1, r_2, ..., r_p)$ according to the P,
Step 3: Find the $\{X_i : i \in I_p\}$ and the module m_i for each X_i,
Step 4: Find the $\beta_i(x_t)$ for $x_t \in X_i$ $t \in I_{a_i}$ and $i \in I_p$,
Step 5: Find the $\alpha^{-1}(x_t)$ for $x_t \in X_i$, $t \in I_{a_i}$ and $i \in I_p$,
Step 6: Find the $\gamma(x)$ for $x \in U$.

Example 19. Let

$$U = \{\text{ç, d, e, f, g, ğ, h, ı, a, b, c, m, n, i, j, k, l, u, ü, o, ö, p,r, s, ş, t, z, v, y}\}$$

and

$$X = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, ..., x_{29}\}$$

Then,

Step 1: By using the algorithm of fragmentation, we can obtain the fragment number $p = 4$ and the $P = (11, 6, 9, 3)$ where $a_1 = 11$, $a_2 = 6$, $a_3 = 9$ and $a_4 = 3$.

Step 2: For $a_1 = 11$, $a_2 = 6$, $a_3 = 9$ and $a_4 = 3$ the rotation key is obtained as $R = (3, 4, 7, 2)$ since $0 < r_1 = 3 < a_1 = 11, \quad 0 < r_2 = 4 < a_2 = 6, \quad 0 < r_3 = 7 < a_3 = 9, \quad 0 < r_1 = 2 < a_4 = 3$.

Step 3: For a_i $(i = 1, 2, 3, 4)$ the fragments of X, X_i, are obtained as,

$$\begin{array}{ll} \text{for } a_1 = 11, & X_1 = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}\} \\ \text{for } a_2 = 6, & X_2 = \{x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}\} \\ \text{for } a_3 = 9, & X_3 = \{x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}\} \\ \text{for } a_4 = 3, & X_4 = \{x_{27}, x_{28}, x_{29}\} \end{array}$$

and value of m_i $(i = 0, 1, 2, 3, 4)$ can also choose as,

$$\begin{array}{ll} \text{for } i = 0, & m_0 = 0 \\ \text{for } i = 1, & m_1 = (m_0 = 0) + (a_1 = 11) = 11 \\ \text{for } i = 2, & m_2 = (m_1 = 11) + (a_2 = 6) = 17 \\ \text{for } i = 3, & m_3 = (m_2 = 17) + (a_3 = 9) = 26 \\ \text{for } i = 4, & m_4 = (m_3 = 26) + (a_4 = 3) = 29. \end{array}$$

Step 4: For $i = 1, 2, 3, 4$ values of the X_i-rotation function β_i are obtained as follows. Here, we first obtain the values of β_1 as,

$$\begin{array}{ll} \beta_1(x_1) = x_4, & \text{since } 1 + r_1 = 1 + 3 = 4 \text{ because of } 1 + 3 < 11 \\ \beta_1(x_2) = x_5, & \text{since } 2 + r_1 = 1 + 3 = 5 \text{ because of } 2 + 3 < 11 \\ \beta_1(x_3) = x_6, & \text{since } 3 + r_1 = 1 + 3 = 6 \text{ because of } 3 + 3 < 11 \\ \beta_1(x_4) = x_7, & \text{since } 4 + r_1 = 1 + 3 = 7 \text{ because of } 4 + 3 < 11 \\ \beta_1(x_5) = x_8, & \text{since } 5 + r_1 = 1 + 3 = 8 \text{ because of } 5 + 3 < 11 \\ \beta_1(x_6) = x_9, & \text{since } 6 + r_1 = 1 + 3 = 9 \text{ because of } 6 + 3 < 11 \\ \beta_1(x_7) = x_{10}, & \text{since } 7 + r_1 = 1 + 3 = 10 \text{ because of } 7 + 3 < 11 \\ \beta_1(x_8) = x_{11}, & \text{since } 8 + r_1 = 1 + 3 = 11 \text{ because of } 8 + 3 = 11 \\ \beta_1(x_9) = x_1, & \text{since } (9 + 3)(mod\, 11) + 0 = 1 \text{ because of } 9 + 3 > 11 \\ \beta_1(x_{10}) = x_2, & \text{since } (10 + 3)(mod\, 11) + 0 = 2 \text{ because of } 10 + 3 > 11 \\ \beta_1(x_{11}) = x_3, & \text{since } (11 + 3)(mod\, 11) + 0 = 3 \text{ because of } 11 + 3 > 11 \end{array}$$

and for $i = 2, 3, 4$ the values of β_i are obtained similarly. Hence

X_1	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}
β_1	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
X_1	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_1	x_2	x_3

X_2	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}	x_{17}
β_2	↓	↓	↓	↓	↓	↓
X_2	x_{16}	x_{17}	x_{12}	x_{13}	x_{14}	x_{15}

X_3	x_{18}	x_{19}	x_{20}	x_{21}	x_{22}	x_{23}	x_{24}	x_{25}	x_{26}
β_3	↓	↓	↓	↓	↓	↓	↓	↓	↓
X_3	x_{25}	x_{26}	x_{18}	x_{19}	x_{20}	x_{21}	x_{22}	x_{23}	x_{24}

X_4	x_{27}	x_{28}	x_{29}
β_4	↓	↓	↓
X_4	x_{29}	x_{27}	x_{28}

and therefore,

X	x_1	x_2	...	x_{11}	x_{12}	x_{13}	...	x_{17}	x_{18}	x_{19}	...	x_{26}	x_{27}	x_{28}	x_{29}
β	↓	↓		↓	↓	↓		↓	↓	↓		↓	↓	↓	↓
X	x_4	x_5	...	x_3	x_{16}	x_{17}	...	x_{15}	x_{25}	x_{26}	...	x_{24}	x_{29}	x_{27}	x_{28}

Step 5: Values of the characterization function α^{-1} are obtained as following list:

X	x_4	x_5	...	x_3	x_{16}	x_{17}	...	x_{15}	x_{25}	x_{26}	...	x_{24}	x_{29}	x_{27}	x_{28}
α^{-1}	↓	↓		↓	↓	↓		↓	↓	↓		↓	↓	↓	↓
U	ç	d	...	c	m	n	...	l	u	ü	...	t	z	v	y

Step 6: Values of the encryption function γ are obtained as following list:

U	a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	...	v	y	z
γ	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓		↓	↓	↓
U	ç	d	e	f	g	ğ	h	ı	a	b	c	m	n	o	i	j	k	...	z	v	y

In this example we showed that the plaintext "ankara" is encrypted as "çliçöç" according to the method which can be seen in Figure 1.

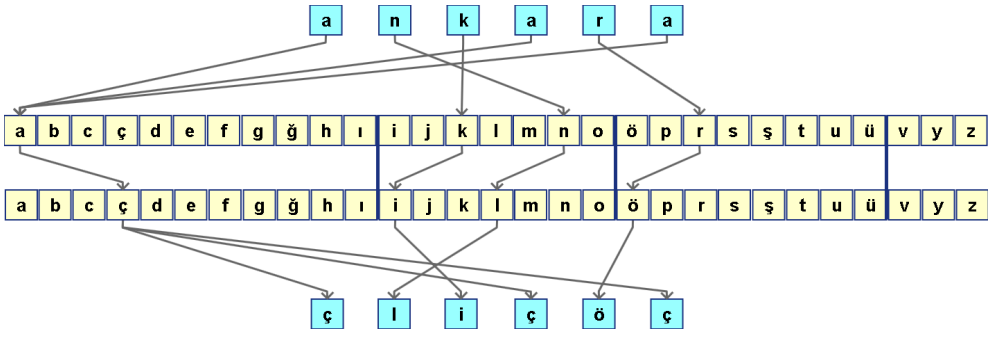


Figure 1: Encryption of "ankara" by FCEA

2.3 FCC-Decryption Algorithm

Assume that U is a character set and X is an indexed character set. Then, an algorithm of the FCC-Decryption is set up as follows:

Algorithm of FCC-Decryption:

Step 1: Use the $\{X_i : i \in I_p\}$ and the module m_i for each X_i,
Step 2: Find the $\beta_i^{-1}(x_t)$ for $x_t \in X_i$, $t \in I_{a_i}$ and $i \in I_p$,
Step 3: Find the $\alpha^{-1}(x)$ for $x \in U$,
Step 4: Find the $\gamma^{-1}(x)$ for $x \in U$.

Example 20. Let us consider the result of Example 19 where

$$U = \{\text{ç, d, e, f, g, ğ,h, ı, a, b, c, m, n, i, j, k, l, u, ü, o, ö, p, r, s, ş, t, z, v, y}\}$$

and

$$X = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, ..., x_{29}\}$$

Then,

Step 1 : In Example 19, for a_i $(i = 1, 2, 3, 4)$ the fragments of X, X_i, and was obtained as

$$\begin{array}{ll} \text{for } a_1 = 11, & X_1 = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}\} \\ \text{for } a_2 = 6, & X_2 = \{x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}\} \\ \text{for } a_3 = 9, & X_3 = \{x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}\} \\ \text{for } a_4 = 3, & X_4 = \{x_{27}, x_{28}, x_{29}\} \end{array}$$

and value of m_i $(i = 0, 1, 2, 3, 4)$ was also choosen as,

$$\begin{array}{ll} \text{for } i = 0, & m_0 = 0 \\ \text{for } i = 1, & m_1 = (m_0 = 0) + (a_1 = 11) = 11 \\ \text{for } i = 2, & m_2 = (m_1 = 11) + (a_2 = 6) = 17 \\ \text{for } i = 3, & m_3 = (m_2 = 17) + (a_3 = 9) = 26 \\ \text{for } i = 4, & m_4 = (m_3 = 26) + (a_4 = 3) = 29 \end{array}$$

Step 2 : For $i = 1, 2, 3, 4$ values of the X_i-rotation function β_i^{-1} are obtained as follows. Here, we first obtain the values of β_1^{-1} as,

$$\begin{array}{ll} \beta_1^{-1}(x_1) = x_9, & \text{since } 1 + m_1 - r_1 = 1 + 11 - 3 = 9 \text{ because of } 1 + 11 - 3 < 11 \\ \beta_1^{-1}(x_2) = x_{10}, & \text{since } 2 + m_1 - r_1 = 2 + 11 - 3 = 10 \text{ because of } 2 + 11 - 3 < 11 \\ \beta_1^{-1}(x_3) = x_{11}, & \text{since } 3 + m_1 - r_1 = 3 + 11 - 3 = 11 \text{ because of } 3 + 11 - 3 = 11 \\ \beta_1^{-1}(x_4) = x_1, & \text{since } (4 + 11 - 3)(mod\,11) + 0 = 1 \text{ because of } 4 + 11 - 3 > 11 \\ \beta_1^{-1}(x_5) = x_2, & \text{since } (5 + 11 - 3)(mod\,11) + 0 = 2 \text{ because of } 5 + 11 - 3 > 11 \\ \beta_1^{-1}(x_6) = x_3, & \text{since } (6 + 11 - 3)(mod\,11) + 0 = 3 \text{ because of } 6 + 11 - 3 > 11 \\ \beta_1^{-1}(x_7) = x_4, & \text{since } (7 + 11 - 3)(mod\,11) + 0 = 4 \text{ because of } 7 + 11 - 3 > 11 \\ \beta_1^{-1}(x_8) = x_5, & \text{since } (8 + 11 - 3)(mod\,11) + 0 = 5 \text{ because of } 8 + 11 - 3 > 11 \\ \beta_1^{-1}(x_9) = x_6, & \text{since } (9 + 11 - 3)(mod\,11) + 0 = 6 \text{ because of } 9 + 11 - 3 > 11 \\ \beta_1^{-1}(x_{10}) = x_7, & \text{since } (10 + 11 - 3)(mod\,11) + 0 = 7 \text{ because of } 10 + 11 - 3 > 11 \\ \beta_1^{-1}(x_{11}) = x_8, & \text{since } (11 + 11 - 3)(mod\,11) + 0 = 8 \text{ because of } 11 + 11 - 3 > 11 \end{array}$$

and for $i = 2, 3, 4$ the values of β_i^{-1} are obtained similarly. Hence,

X_1	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}
β_1^{-1}	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
X_1	x_9	x_{10}	x_{11}	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8

X_2	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}	x_{17}
β_2^{-1}	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
X_2	x_{14}	x_{15}	x_{16}	x_{17}	x_{12}	x_{13}

X_3	x_{18}	x_{19}	x_{20}	x_{21}	x_{22}	x_{23}	x_{24}	x_{25}	x_{26}
β_3^{-1}	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
X_3	x_{20}	x_{21}	x_{22}	x_{23}	x_{24}	x_{25}	x_{26}	x_{18}	x_{19}

X_4	x_{27}	x_{28}	x_{29}
β_4^{-1}	$\downarrow$	$\downarrow$	$\downarrow$
X_4	x_{29}	x_{27}	x_{28}

and therefore,

X	x_1	x_2	...	x_{11}	x_{12}	x_{13}	...	x_{17}	x_{18}	x_{19}	...	x_{26}	x_{27}	x_{28}	x_{29}
β^{-1}	$\downarrow$	$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
X	x_9	x_{10}	...	x_8	x_{14}	x_{15}	...	x_{13}	x_{20}	x_{21}	...	x_{19}	x_{29}	x_{27}	x_{28}

Step 3: Values of the characterization function α^{-1} are obtained as following list:

X	x_9	x_{10}	...	x_8	x_{14}	x_{15}	...	x_{13}	x_{20}	x_{21}	...	x_{19}	x_{29}	x_{27}	x_{28}
α^{-1}	$\downarrow$	$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
U	a	b	...	ı	i	j	...	n	o	ö	...	ü	v	y	z

Step 4: Values of the decryption function γ^{-1} are obtained as following list:

U	ç	d	e	f	g	ğ	h	ı	a	b	c	m	n	o	i	j	k	...	z	v	y
γ^{-1}	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$
U	a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	...	v	y	z

In this example we showed that the ciphertext "çliçöç" is decrypted as "ankara".

3 FC Encryption Program Codes

In this section, the FCC-method is programmed by using C# as follows:

```
private static string[] alf_tex()
{
   string[] alphabet = { "a", "b",..,"Y", "Z"}; //caharacter set
   return alpabet;
}
private static int _rnd(int bas, int bit)
```

```
{
   Random rnd = new Random();
   int deger = rnd.Next(bas, bit);
   return deger;
}
private static string _key(int alphabet_number)
{
   string key = "";
   int n = alphabet_number;
   int a,r;
   do
   {
       if (n >= 6)
       {
           a = _rnd(3, n - 3); //Fragment key
       }
       else
       {
           a = n;
       }
       r = _rnd(2, a);//Rotation key
       key += a.ToString() + "," + r.ToString() + '-';
       n = n - a;
   }
   while (n > 0);
   return key;
}
private void btn_creat_alphabet_Click(object sender, EventArgs e)
{
   //key function
   if (rdsifre.Checked)
   {
       string key = _key(alp_tex().Length);
       txtanahtar.Text = key;
   }
   int alfabe_sayac = 1;
   string[] fragment = key.Substring(0,key.Length-1).Split('-');
   string[][] U = new string[fragment.Length][];//(Açık U)
   string[][] SU = new string[fragment.Length][];//(encrypted U)
   //be divided into sets of the alphabet
   for (int j = 0; j < parca.Length; j++)
   {
       string[] parca_a = fragment[j].ToString().Split(',');
```

```
        int P = int.Parse(fragment_a[0]); //fragment key
        U[j] = new string[alp_tex().Length + 1];
        SU[j] = new string[alp_tex().Length + 1];
        for (int x = 0; x < P; x++)
        {
            U[j][alfabe_sayac] = alp_tex()[alphabet_sayac - 1];
            alphabet_sayac++;
        }
    }
    //encrypting alphabet
    int m = 0;
    int index = 1;
    for (int j = 0; j < U.Length; j++)
    {
        string[] parca_a = fragment[j].ToString().Split(',');
        int P = int.Parse(fragment_a[0]); //fragment key
        int R = int.Parse(fragment_a[1]); //rotation key
        m += P;
        for (int x = 0; x < P; x++)
        {
            int k = 0;
            if ((index + R) <= m) //rotation function
            {
                k = index + R;
            }
            else if ((index + R) > m)
            {
                k = ((index + R) % m) + (m - P);
            }
            SU[j][index] = U[j][k];
            index++;
        }
    }
}
```

4 Conclusions

In this work, a cipher method so called fragmented Caesar cipher method is defined. A mathematical modeling and then a computer programs of the method have done. The method is based on the basic logic of Caesar cipher. The classical Caesar cipher is a type of substitution cipher in which each letter is replaced by a letter some

fixed number of positions in the alphabet. The Fragmented Caesar cipher has more possibility then the classical Caesar cipher because of the fragmented alphabet is used to cipher. We finally give an example to show the cipher method is working successfully.

References

[1] Y. Aydoğan, Multi Fragmented Caesar Cipher Method and its Applications (In Turkish), MSc Thesis, Gaziosmanpasa University, Graduate School of Natural and Applied Science, 2014.

[2] S. Dey, Nath and A. J. Nath, An Integrated Symmetric Key Cryptographic Method - Amalgamation of TTJSA Algorithm , Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal Method: SJA Algorithm, I. J. Modern Edu. and Comp. Sci., 5 (2012), 1-9.

[3] J. Hoffstein, J. Pipher and J. H. Silverman, An Introduction to Mathematical Cryptograph, Springer-Newyork, 2008.

[4] A. Mishra, Enhancing Security of Caesar Cipher Using Different Methods, I. J. of Res. in Eng. and Tech., 2(9) (2013), 954-959.

[5] O. E. Omolara, A. I. Oludare and S. E. Abdulahi, Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication, Comp. Eng. and I. Syst., 5(5) (2014).

[6] C. Paar, J. Pelzl, Understanding Cryptograph, Springer-Verlag, 2010.

[7] P. Patni, A Poly-alphabetic Approach to Caesar Cipher Algorithm, I. J. of Comp. Sci. and Info. Tech., 4(6) (2013), 954-959.

[8] P. Patni, Implementation and Result Analysis of Polyalphabetic Approach to Caesar Cipher, IOSR J. of Com. Eng., 16(4) (2014), 100-106.

[9] A. Sinkov, Elementary Cryptanalysis – A Mathematical Approach, New Mathematical Library, No. 22, Mathematical Association of America, 1966.

http://www.newtheory.org **ISSN: 2149-1402**

Journal of New Theory

Received: 14.01.2016 *Year*: **2016**, *Number*: **14**, *Pages*: **58-72**
Published: 24.07.2016 *Original Article*[**]

FRAGMENTED POLYALPHABETIC CIPHER

Yunus Aydoğan <yunus.programmer@gmail.com>
Naim Çağman <naim.cagman@gop.edu.tr>
Irfan Şimşek[*] <irfan.simsek@gop.edu.tr>

Department of Mathematics, Faculty of Arts and Sciences, Gaziosmanpaşa University
60240 Tokat, Turkey

Abstract — In this study, we define a polyalphabetic cipher method that is called fragmented polyalphabetic (FP) cipher that is based on the fragmented Caesar (FC) cipher. In the FP-cipher, plaintext is encrypted by multiple encryption alphabets which are obtained by using the FC-cipher. We then construct a mathematical modeling and make a computer program of the method.

Keywords — *Encryption, Decryption, Cipher, Polyalphabetic Cipher, Fragmented Polyalphabetic Cipher.*

1 Introduction

One of the earliest well known cryptographic systems was used by Julius Caesar [5]. In Caesar cipher that is a simple substitution cipher and an example of monoalphabetic cipher, each letter in the plaintext is shifted by a letter a certain number of positions down the alphabet. The Caesar cipher can be decrypted in an easy way with the brute-force attack [4]. One of the first polyalphabetic ciphers called Vigenere cipher dates back to the 16th century. This cipher was named after Vigenere (1523-1596). The Vigenere cipher works by using different shift ciphers to encrypt different letters [3].

Aydoğan et al. [1] defined the fragmented Caesar (FC) cipher which is based on the basic logic of Caesar cipher. The FC-cipher has more possibility then the classical Caesar cipher because of the fragmented alphabet is used to cipher. They also construct a mathematical modeling and make a computer program of the FC-cipher.

In this study, we define a polyalphabetic cipher that is called fragmented polyalphabetic (FP) cipher. The FP-cipher is based on the FC-cipher. The FP-cipher is

[**] *Edited by* Oktay Muhtaroğlu *(Area Editor)*
[*] *Corresponding Author.*

also generalized of the Vigenere cipher. In the FC-cipher, the alphabet is broken into small fragments and each letter is replaced by a letter some arbitrary number of positions down in each fragment. The FP-cipher uses different alphabets that are obtained by using the FC-cipher to encrypt different letters. We then construct a mathematical modeling and make a computer program of this cipher method.

The present paper is a condensation of part of the dissertation [2].

2 Preliminary

In this section, we give definitions and properties of the FC-cipher which are taken directly from [1].

2.1 Mathematical Model of FC-cipher

Throughout this paper, ASCII (**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange) is used, $I_n = \{1, 2, ..., n\}$ for all $n \in \mathbb{N}$ is an index set and U is a set of using characters which is ordered according to the ASCII.

Definition 1. Let $|U| = n$ and $X = \{x_i : i \in I_n\}$ be an ordered set according to the index set I_n. Then,

$$\alpha : U \to X, \quad \alpha(i\text{-th element}) = x_i, i \in I_n,$$

is called **indexing function** of U. Here, x_i is called **indexed element** of ith element of U and the set X is called **indexed character set** of U.

Example 2. Let 1, 9, b, M, $<$ and $+$ be using characters. Then, the character set U is written as $U = \{+, 1, 9, <, M, b\}$ since

x	$+$	1	9	$<$	M	b
$ASCII$	43	49	57	60	77	98

Therefore the indexed character set of U is obtained as $X = \{x_1, x_2, x_3, x_4, x_5, x_6\}$ since

x	$+$	1	9	$<$	M	b
$\alpha(x)$	x_1	x_2	x_3	x_4	x_5	x_6

Definition 3. Let X be an indexed character set and $|X| = n$. Then, for $a_p \in \mathbb{N}$, $p \in I_n$, a fragmentation algorithm is set up as follows:

Algorithm of Fragmentation:

Step 1: Choose a_1 such that $2 \leq a_1 \leq n_1 = n - 2$

Step 2: Let $n_2 = n_1 - a_1$. If $n_2 > 4$, choose a_2 such that $2 \leq a_2 \leq n_2 - 2$, if not $a_2 = n_2$ which means the process is terminated.

$\vdots$

Step p: Let $n_p = n_{p-1} - a_{p-1}$. If $n_p > 4$, choose a_p such that $2 \leq a_p \leq n_p - 2$, if not $a_p = n_p$ which means the process is terminated.

Here, p is called a **fragment number**, a_p is number of characters in a fragment and $P = (a_1, a_2, ..., a_p)$ is called **fragment key** of X.

We can briefly choose values a_p as follow, for $p \in I_n$ and $i \in I_p$,

$$\begin{cases} 2 \leq a_1 \leq n_1, & \text{if } p = 1,\ n_1 = n - 2 \\ 2 \leq a_p \leq n_i - 2, & \text{if } p > 1,\ 4 < n_p,\ n_p = n_{p-1} - a_{p-1} \\ n_p = a_p, & \text{if } p > 1,\ n_p < 4,\ n_p = n_{p-1} - a_{p-1} \end{cases}$$

Example 4. Let X be an indexed character set and $|X| = 13$. If the fragmentation algorithm is working as follows,

Step 1: Choose $a_1 = 5$ such that $2 \leq a_1 \leq n_1 = 13 - 2 = 11$,

Step 2: Choose $a_2 = 6$ such that $2 \leq a_2 \leq 8 - 2$, because of $n_2 = 13 - 5 = 8$ and $8 > 4$,

Step 3: Choose $a_3 = 2$ because of $n_3 = 8 - 6 = 2$ and $2 < 4$.

Then, we obtain that $p = 3$ and $P = (5, 6, 2)$.

Definition 5. Let $X = \{x_1, x_2, ..., x_n\}$ be an indexed character set. For all $i \in I_n$ and $k \in I_{n-i}$, the set $W = \{x_i, x_{i+1}, ..., x_{i+k}\}$ is called as a **block subset** of X and denoted by $W \sqsubseteq X$.

Definition 6. Let X be an indexed character set, p be a number of fragment of X. If $X_i \sqsubseteq X$ has the following conditions, then family of set $\{X_i : i \in I_p\}$ is called an **ordered fragmentation** of X.

1. $|X_i| = a_i$,
2. $X_i \cap X_j = \emptyset$ for $i, j \in I_p$, $i \neq j$,
3. $X = \bigcup_{i \in I_p} X_i$,
4. $x_{max(X_i)+1} = x_{min(X_{i+1})}$ for $i \in I_p$, where $x_{min(X_i)}$ and $x_{max(X_i)}$ be the first and the last element of X_i, respectively.

Here, the X_i is called a **fragment** of X for $i \in I_p$.

Example 7. Let us consider Example 4 where $X = \{x_1, x_2, ..., x_{13}\}$ and $P = (5, 6, 2)$. Then, for $a_1 = 5$, $a_2 = 6$ and $a_3 = 2$ the ordered fragmentation of X are respectively as follow,

$$\begin{aligned} X_1 &= \{x_1, x_2, x_3, x_4, x_5\} \\ X_2 &= \{x_6, x_7, x_8, x_9, x_{10}, x_{11}\} \\ X_3 &= \{x_{12}, x_{13}\} \end{aligned}$$

Therefor, the ordered fragmentation of X is obtained as $\{X_1, X_2, X_3\}$.

Definition 8. Let X_i be a fragment of X and a_i be the number of X_i for all $i \in I_p$. If $0 < r_i < a_i$, then $R = (r_1, r_2, ..., r_p)$ is called **rotation key** of X.

Here, the r_i is called a **number of rotation** of X_i for all $i \in I_p$.

Note that the key of this method has two part, one of them is a fragment key P and the other is a rotation key R.

Example 9. Let us consider Example 4, if we choose number of rotations $r_1 = 3$, $r_2 = 4$ and $r_3 = 1$ for X_1, X_2, X_3, respectively. Then, the rotation key of X would be $R = (3, 4, 1)$.

Definition 10. Let X be an indexed character set, $\{X_1, X_2, ..., X_p\}$ be an ordered fragmentation of X and $P = (a_1, a_2, ..., a_p)$ be a fragment key of X. Then, m_i is defined by

$$m_i = \begin{cases} 0, & i = 0 \\ m_{i-1} + a_i, & i \in I_p \end{cases}$$

and called a **module** of X_i for all $i \in I_p$.

It is clear to see that $x_{m_i} = x_{max(X_i)}$ for $i \in I_p$.

Definition 11. Let X be an indexed character set and $\{X_1, X_2, ..., X_p\}$ be an ordered fragmentation of X. If m_i is a module of X_i for all $i \in I_p$ and $R = (r_1, r_2, ..., r_p)$ is a rotation key of X, then **X_i-rotation function**, denoted by β_i, is defined by

$$\beta_i : X_i \to X_i,\ \beta_i(x_t) = \begin{cases} x_{t+r_i}, & t + r_i \leq m_i \\ x_{(t+r_i)(mod\, m_i)+m_{i-1}}, & t + r_i > m_i \end{cases}$$

where $t \in I_{a_i}$.

Definition 12. Let X be an indexed character set and $\{X_1, X_2, ..., X_p\}$ be an ordered fragmentation of X. If β_i is an X_i-rotation function for all $i \in I_p$, then the following function

$$\beta : X \to X,\ \beta(x) = \begin{cases} \beta_1(x), & x \in X_1 \\ \beta_2(x), & x \in X_2 \\ \quad \vdots & \\ \beta_p(x), & x \in X_p \end{cases}$$

is called a **rotation function** of X.

Definition 13. Let $\alpha : U \to X$ be an indexing function. Then for all $t \in I_n$, inverse of α is called a **characterization function** and defined by

$$\alpha^{-1} : X \to U, \quad \alpha^{-1}(x_t) = \text{"}t\text{-th element of U "}$$

Definition 14. If $\alpha : U \to X$, $\alpha^{-1} : X \to U$ and $\beta : X \to X$ be indexing, characterization and rotation functions, respectively, then an **encryption function** on U is defined by

$$\gamma : U \to U, \quad \gamma(x) = \alpha^{-1}(\beta(\alpha(x)))$$

Definition 15. Let X be an indexed character set and $\{X_1, X_2, ..., X_p\}$ be an ordered fragmentation of X. If $R = (r_1, r_2, ..., r_p)$ is a rotation key of X, $\beta_i : X_i \to X_i$ is an X_i-rotation function and m_i is a module of X_i for all $i \in I_p$, then **inverse of rotation function** of X_i, denoted by β_i^{-1}, is defined by

$$\beta_i^{-1} : X_i \to X_i,$$
$$\beta_i^{-1}(x_t) = \begin{cases} x_{t+m_i-(r_i+m_{i-1})}, & t + m_i - (r_i + m_{i-1}) \leq m_i \\ x_{(t+m_i-(r_i+m_{i-1}))(mod\, m_i)+m_{i-1}}, & t + m_i - (r_i + m_{i-1}) > m_i \end{cases} \text{ where } t \in I_{a_i}.$$

Definition 16. Let X be an indexed character set and $\{X_1, X_2, ..., X_p\}$ be an ordered fragmentation of X. If β_i^{-1} is an inverse of rotation function of X_i for all $i \in I_p$, then the following function

$$\beta^{-1} : X \to X,\ \beta^{-1}(x) = \begin{cases} \beta_1^{-1}(x), & x \in X_1 \\ \beta_2^{-1}(x), & x \in X_2 \\ \quad \vdots & \\ \beta_p^{-1}(x), & x \in X_p \end{cases}$$

is called a **inverse of rotation function** of X.

Definition 17. If $\alpha : U \to X$, $\alpha^{-1} : X \to U$, $\beta^{-1} : X \to X$ and $\gamma : U \to U$ be indexing, characterization, inverse of rotation and encryption functions, respectively, then a **decryption function** on U is defined by

$$\gamma^{-1} : U \to U, \quad \gamma^{-1}(x) = \alpha^{-1}(\beta^{-1}(\alpha(x)))$$

It is clear to see that $\gamma^{-1}(x) = \alpha^{-1}(\beta^{-1}((\alpha^{-1})^{-1}(x))) = \alpha^{-1}(\beta^{-1}(\alpha(x)))$.

Definition 18. Let U be a character set, P be a fragment key, R be a rotation key and γ be an encryption function. The four tuple (U, P, R, γ) is called an **FC-cipher encryption** on U. The four tuple (U, P, R, γ^{-1}) is called an **FC-cipher decryption** on U.

2.2 FC-cipher Encryption Algorithm

In this subsection, we give the algorithm of FC-cipher.

Assume that U is a character set and X is an indexed character set. Then, an algorithm of the FC-cipher encryption is set up as follows:

Algorithm of FC-cipher Encryption:

Step 1: Find the fragment number p and the $P = (a_1, a_2, ..., a_p)$,
Step 2: Choose the $R = (r_1, r_2, ..., r_p)$ according to the P,
Step 3: Find the $\{X_i : i \in I_p\}$ and the module m_i for each X_i,
Step 4: Find the $\beta_i(x_t)$ for $x_t \in X_i$ $t \in I_{a_i}$ and $i \in I_p$,
Step 5: Find the $\alpha^{-1}(x_t)$ for $x_t \in X_i$, $t \in I_{a_i}$ and $i \in I_p$,
Step 6: Find the $\gamma(x)$ for $x \in U$.

Example 19. Let

$$U = \{\text{ç, d, e, f, g, ğ, h, ı, a, b, c, m, n, i, j, k, l, u, ü, o, ö, p,r, s, ş, t, z, v, y}\}$$

and

$$X = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, ..., x_{29}\}$$

Then,

Step 1: By using the algorithm of fragmentation, we can obtain the fragment number $p = 4$ and the $P = (11, 6, 9, 3)$ where $a_1 = 11$, $a_2 = 6$, $a_3 = 9$ and $a_4 = 3$.

Step 2: For $a_1 = 11$, $a_2 = 6$, $a_3 = 9$ and $a_4 = 3$ the rotation key is obtained as $R = (3, 4, 7, 2)$ since $0 < r_1 = 3 < a_1 = 11, \quad 0 < r_2 = 4 < a_2 = 6, \quad 0 < r_3 = 7 < a_3 = 9, \quad 0 < r_1 = 2 < a_4 = 3$.

Step 3: For a_i $(i = 1, 2, 3, 4)$ the fragments of X, X_i, are obtained as,

$$\begin{array}{ll} \text{for } a_1 = 11, & X_1 = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}\} \\ \text{for } a_2 = 6, & X_2 = \{x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}\} \\ \text{for } a_3 = 9, & X_3 = \{x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}\} \\ \text{for } a_4 = 3, & X_4 = \{x_{27}, x_{28}, x_{29}\} \end{array}$$

and value of m_i $(i = 0, 1, 2, 3, 4)$ can also choose as,

$$\begin{array}{ll} \text{for } i = 0, & m_0 = 0 \\ \text{for } i = 1, & m_1 = (m_0 = 0) + (a_1 = 11) = 11 \\ \text{for } i = 2, & m_2 = (m_1 = 11) + (a_2 = 6) = 17 \\ \text{for } i = 3, & m_3 = (m_2 = 17) + (a_3 = 9) = 26 \\ \text{for } i = 4, & m_4 = (m_3 = 26) + (a_4 = 3) = 29. \end{array}$$

Step 4: For $i = 1, 2, 3, 4$ values of the X_i-rotation function β_i are obtained as follows. Here, we first obtain the values of β_1 as,

$$\begin{array}{ll} \beta_1(x_1) = x_4, & \text{since } 1 + r_1 = 1 + 3 = 4 \text{ because of } 1 + 3 < 11 \\ \beta_1(x_2) = x_5, & \text{since } 2 + r_1 = 1 + 3 = 5 \text{ because of } 2 + 3 < 11 \\ \beta_1(x_3) = x_6, & \text{since } 3 + r_1 = 1 + 3 = 6 \text{ because of } 3 + 3 < 11 \\ \beta_1(x_4) = x_7, & \text{since } 4 + r_1 = 1 + 3 = 7 \text{ because of } 4 + 3 < 11 \\ \beta_1(x_5) = x_8, & \text{since } 5 + r_1 = 1 + 3 = 8 \text{ because of } 5 + 3 < 11 \\ \beta_1(x_6) = x_9, & \text{since } 6 + r_1 = 1 + 3 = 9 \text{ because of } 6 + 3 < 11 \\ \beta_1(x_7) = x_{10}, & \text{since } 7 + r_1 = 1 + 3 = 10 \text{ because of } 7 + 3 < 11 \\ \beta_1(x_8) = x_{11}, & \text{since } 8 + r_1 = 1 + 3 = 11 \text{ because of } 8 + 3 = 11 \\ \beta_1(x_9) = x_1, & \text{since } (9 + 3)(mod\, 11) + 0 = 1 \text{ because of } 9 + 3 > 11 \\ \beta_1(x_{10}) = x_2, & \text{since } (10 + 3)(mod\, 11) + 0 = 2 \text{ because of } 10 + 3 > 11 \\ \beta_1(x_{11}) = x_3, & \text{since } (11 + 3)(mod\, 11) + 0 = 3 \text{ because of } 11 + 3 > 11 \end{array}$$

and for $i = 2, 3, 4$ the values of β_i are obtained similarly. Hence

X_1	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}
β_1	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
X_1	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_1	x_2	x_3

X_2	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}	x_{17}
β_2	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
X_2	x_{16}	x_{17}	x_{12}	x_{13}	x_{14}	x_{15}

X_3	x_{18}	x_{19}	x_{20}	x_{21}	x_{22}	x_{23}	x_{24}	x_{25}	x_{26}
β_3	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
X_3	x_{25}	x_{26}	x_{18}	x_{19}	x_{20}	x_{21}	x_{22}	x_{23}	x_{24}

X_4	x_{27}	x_{28}	x_{29}
β_4	$\downarrow$	$\downarrow$	$\downarrow$
X_4	x_{29}	x_{27}	x_{28}

and therefore,

X	x_1	x_2	...	x_{11}	x_{12}	x_{13}	...	x_{17}	x_{18}	x_{19}	...	x_{26}	x_{27}	x_{28}	x_{29}
β	↓	↓		↓	↓	↓		↓	↓	↓		↓	↓	↓	↓
X	x_4	x_5	...	x_3	x_{16}	x_{17}	...	x_{15}	x_{25}	x_{26}	...	x_{24}	x_{29}	x_{27}	x_{28}

Step 5: Values of the characterization function α^{-1} are obtained as following list:

X	x_4	x_5	...	x_3	x_{16}	x_{17}	...	x_{15}	x_{25}	x_{26}	...	x_{24}	x_{29}	x_{27}	x_{28}
α^{-1}	↓	↓		↓	↓	↓		↓	↓	↓		↓	↓	↓	↓
U	ç	d	...	c	m	n	...	l	u	ü	...	t	z	v	y

Step 6: Values of the encryption function γ are obtained as following list:

U	a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	...	v	y	z
γ	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓		↓	↓	↓
U	ç	d	e	f	g	ğ	h	ı	a	b	c	m	n	o	i	j	k	...	z	v	y

In this example we showed that the plaintext "ankara" is encrypted as "çliçöç" according to the method which can be seen in Figure 1.

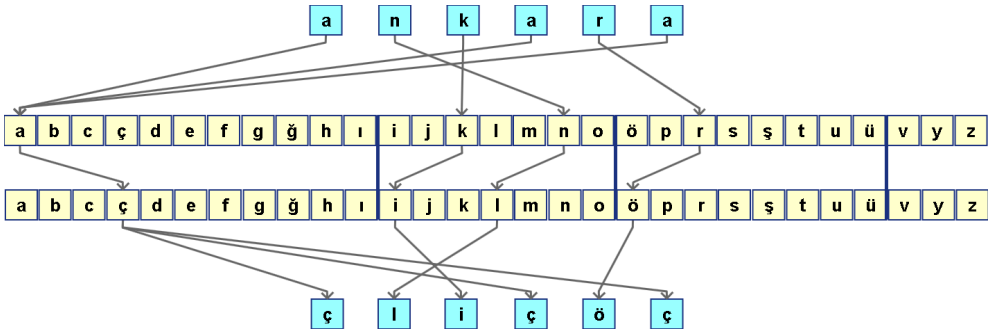


Figure 1: Encryption of "ankara" by FCEA

2.3 FC-cipher Decryption Algorithm

In this subsection, we give the algorithm of FC-cipher decryption method.

Assume that U is a character set and X is an indexed character set. Then, an algorithm of the FC-cipher decryption is set up as follows:

Algorithm of FC-cipher Decryption:

Step 1: Use the $\{X_i : i \in I_p\}$ and the module m_i for each X_i,
Step 2: Find the $\beta_i^{-1}(x_t)$ for $x_t \in X_i$, $t \in I_{a_i}$ and $i \in I_p$,
Step 3: Find the $\alpha^{-1}(x)$ for $x \in U$,
Step 4: Find the $\gamma^{-1}(x)$ for $x \in U$.

Example 20. Let us consider the result of Example 19 where

$$U = \{\text{ç, d, e, f, g, ğ,h, ı, a, b, c, m, n, i, j, k, l, u, ü, o, ö, p, r, s, ş, t, z, v, y}\}$$

and

$$X = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, ..., x_{29}\}$$

Then,

Step 1 : In Example 19, for a_i $(i = 1, 2, 3, 4)$ the fragments of X, X_i, and was obtained as

$$\begin{array}{ll} \text{for } a_1 = 11, & X_1 = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}\} \\ \text{for } a_2 = 6, & X_2 = \{x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}\} \\ \text{for } a_3 = 9, & X_3 = \{x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}\} \\ \text{for } a_4 = 3, & X_4 = \{x_{27}, x_{28}, x_{29}\} \end{array}$$

and value of m_i $(i = 0, 1, 2, 3, 4)$ was also choosen as,

$$\begin{array}{ll} \text{for } i = 0, & m_0 = 0 \\ \text{for } i = 1, & m_1 = (m_0 = 0) + (a_1 = 11) = 11 \\ \text{for } i = 2, & m_2 = (m_1 = 11) + (a_2 = 6) = 17 \\ \text{for } i = 3, & m_3 = (m_2 = 17) + (a_3 = 9) = 26 \\ \text{for } i = 4, & m_4 = (m_3 = 26) + (a_4 = 3) = 29 \end{array}$$

Step 2 : For $i = 1, 2, 3, 4$ values of the X_i-rotation function β_i^{-1} are obtained as follows. Here, we first obtain the values of β_1^{-1} as,

$$\begin{array}{ll} \beta_1^{-1}(x_1) = x_9, & \text{since } 1 + m_1 - r_1 = 1 + 11 - 3 = 9 \text{ because of } 1 + 11 - 3 < 11 \\ \beta_1^{-1}(x_2) = x_{10}, & \text{since } 2 + m_1 - r_1 = 2 + 11 - 3 = 10 \text{ because of } 2 + 11 - 3 < 11 \\ \beta_1^{-1}(x_3) = x_{11}, & \text{since } 3 + m_1 - r_1 = 3 + 11 - 3 = 11 \text{ because of } 3 + 11 - 3 = 11 \\ \beta_1^{-1}(x_4) = x_1, & \text{since } (4 + 11 - 3)(mod\, 11) + 0 = 1 \text{ because of } 4 + 11 - 3 > 11 \\ \beta_1^{-1}(x_5) = x_2, & \text{since } (5 + 11 - 3)(mod\, 11) + 0 = 2 \text{ because of } 5 + 11 - 3 > 11 \\ \beta_1^{-1}(x_6) = x_3, & \text{since } (6 + 11 - 3)(mod\, 11) + 0 = 3 \text{ because of } 6 + 11 - 3 > 11 \\ \beta_1^{-1}(x_7) = x_4, & \text{since } (7 + 11 - 3)(mod\, 11) + 0 = 4 \text{ because of } 7 + 11 - 3 > 11 \\ \beta_1^{-1}(x_8) = x_5, & \text{since } (8 + 11 - 3)(mod\, 11) + 0 = 5 \text{ because of } 8 + 11 - 3 > 11 \\ \beta_1^{-1}(x_9) = x_6, & \text{since } (9 + 11 - 3)(mod\, 11) + 0 = 6 \text{ because of } 9 + 11 - 3 > 11 \\ \beta_1^{-1}(x_{10}) = x_7, & \text{since } (10 + 11 - 3)(mod\, 11) + 0 = 7 \text{ because of } 10 + 11 - 3 > 11 \\ \beta_1^{-1}(x_{11}) = x_8, & \text{since } (11 + 11 - 3)(mod\, 11) + 0 = 8 \text{ because of } 11 + 11 - 3 > 11 \end{array}$$

and for $i = 2, 3, 4$ the values of β_i^{-1} are obtained similarly. Hence,

X_1	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}
β_1^{-1}	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
X_1	x_9	x_{10}	x_{11}	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8

X_2	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}	x_{17}
β_2^{-1}	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
X_2	x_{14}	x_{15}	x_{16}	x_{17}	x_{12}	x_{13}

X_3	x_{18}	x_{19}	x_{20}	x_{21}	x_{22}	x_{23}	x_{24}	x_{25}	x_{26}
β_3^{-1}	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
X_3	x_{20}	x_{21}	x_{22}	x_{23}	x_{24}	x_{25}	x_{26}	x_{18}	x_{19}

X_4	x_{27}	x_{28}	x_{29}
β_4^{-1}	$\downarrow$	$\downarrow$	$\downarrow$
X_4	x_{29}	x_{27}	x_{28}

and therefore,

X	x_1	x_2	...	x_{11}	x_{12}	x_{13}	...	x_{17}	x_{18}	x_{19}	...	x_{26}	x_{27}	x_{28}	x_{29}
β^{-1}	$\downarrow$	$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
X	x_9	x_{10}	...	x_8	x_{14}	x_{15}	...	x_{13}	x_{20}	x_{21}	...	x_{19}	x_{29}	x_{27}	x_{28}

Step 3 : Values of the characterization function α^{-1} are obtained as following list:

X	x_9	x_{10}	...	x_8	x_{14}	x_{15}	...	x_{13}	x_{20}	x_{21}	...	x_{19}	x_{29}	x_{27}	x_{28}
α^{-1}	↓	↓		↓	↓	↓		↓	↓	↓		↓	↓	↓	↓
U	a	b	...	ı	i	j	...	n	o	ö	...	ü	v	y	z

Step 4 : Values of the decryption function γ^{-1} are obtained as following list:

U	ç	d	e	f	g	ğ	h	ı	a	b	c	m	n	o	i	j	k	...	z	v	y
γ^{-1}	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓		↓	↓	↓
U	a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	...	v	y	z

In this example we showed that the ciphertext "çliçöç" is decrypted as "ankara".

3 Fragmented Polyalphabetic Cipher

In this section, we define a new cipher method which is called fragmented polyalphabetic cipher (FP-cipher) based on the FC-cipher. In the FP-cipher, the plaintext is encrypted by multiple encryption alphabets which are obtained by using the FC-cipher.

From now on, we use $k \in \mathbb{N}$ as a number of encrypted alphabets that are obtained by using the FC-cipher.

3.1 Mathematical Model of FP-cipher

In this subsection, we first give a mathematical model of the FP-cipher. We then write an algorithm of the FP-cipher to make a computer program.

Definition 21. Let U be a character set and $\gamma_i : U \to U$ be an encryption function for all $i \in I_k$. If all of the characters in the plaintext are indexed as $y_1y_2...y_q$ for $q \in \mathbb{N}$, then a k-**multiple encryption function** on U is defined by

$$\delta_k : U \to U, \quad \delta_k(y_t) = \begin{cases} \gamma_i(y_t), & t \equiv i(mod\, k) \\ \gamma_k(y_t), & t \equiv 0(mod\, k) \end{cases}$$

for all $t \in I_q$ and $i \in I_k$.

Definition 22. Let U be a character set and $\gamma_i^{-1} : U \to U$ be an encryption function for all $i \in I_k$. If all of the characters in the ciphertext are indexed as $s_1s_2...s_q$ for $q \in \mathbb{N}$, then a k-**multiple decryption function** on U is defined by

$$\delta_k^{-1} : U \to U, \quad \delta_k^{-1}(s_t) = \begin{cases} \gamma_i^{-1}(s_t), & t \equiv i(mod\, k) \\ \gamma_k^{-1}(s_t), & t \equiv 0(mod\, k) \end{cases}$$

for all $t \in I_q$ and $i \in I_k$.

The Definitions 21 and 22 are demonstrated in Figure 2.

Definition 23. Let U be a character set and P_i be a fragment key, R_i be a rotation key for all $i \in I_k$. Then a k-**multiple fragment key** and k-**multiple rotation key** are defined as follow, respectively

$$P_k = (P_1, P_2, ..., P_k), \quad R_k = (R_1, R_2, ..., R_k).$$

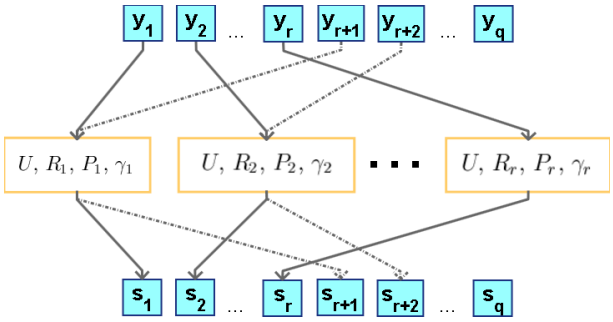


Figure 2: FP-cipher

Definition 24. Let (U, P_i, R_i, γ_i) be an FC-cipher encryption and $(U, P_i, R_i, \gamma_i^{-1})$ be an FC-cipher decryption on U for all $i \in I_k$. Then, each five tuple

$$(U, k, P_k, R_k, \delta_k), \quad (U, k, P_k, R_k, \delta_k^{-1})$$

is called an **FP-cipher encryption** and **FP-cipher decryption** on U, respectively.

3.2 FP-cipher Encryption Algorithm

In this subsection, we give an algorithm of the FP-cipher encryption method.

Assume that all of characters in a plaintext are be indexed as $y_1y_2...y_q$ and k be a number of encrypted alphabets that are obtained by using the FC-cipher. Then, an algorithm of the FP-cipher encryption is set up as follow:

Algorithm of FP-cipher Encryption

Step 1 : Find the $P_k = (P_1, P_2, ..., P_k)$ and $R_k = (R_1, R_2, ..., R_k)$,
Step 2 : Find the values of γ_i for $i \in I_k$,
Step 3 : Find the values $\delta(y_t)$ for all $t \in I_q$.

Example 25. Let

$$U = \{\text{a, b, c, ç, d, e, f, g, ğ, h, ı, i, j, k, l, m, n, o, ö, p, r, s, ş, t, u, ü, v, y, z}\}$$

be a character set and "ankara" be a plaintext. Assume that this plaintext is indexed as $y_1y_2y_3y_4y_5y_6$ and encrypted by 3-FP-cipher encryption. Then,

Step 1 : The P_i and R_i can be obtained by using the FC-cipher as follow,

i	P_i	R_i
1	(11,6,10,2)	(4,2,5,1)
2	(10,9,5,5)	(3,4,2,3)
3	(5,6,4,10,4)	(2,2,1,3,1)

Step 2 : For $i = 1, 2, 3$, the values $\gamma_i(x)$ are obtained as follow,

x	a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l
$\gamma_1(x)$	d	e	f	g	ğ	h	ı	a	b	c	ç	m	n	i	j
$\gamma_2(x)$	ç	d	e	f	g	ğ	h	a	b	c	l	m	n	o	ö
$\gamma_3(x)$	c	ç	d	a	b	g	ğ	h	ı	e	f	j	k	l	i

	m	n	o	ö	p	r	s	ş	t	u	ü	v	y	z
	k	l	ş	t	u	ü	v	o	ö	p	r	s	z	y
	ı	i	j	k	s	ş	t	p	r	y	z	u	ü	v
	ö	p	r	s	ş	t	u	m	n	o	v	y	z	ü

Step 3 : For all $t \in I_6$, the values $\delta(y_t)$ are obtained as follow,

$$\begin{array}{lllll}
\text{for } i=1, & \delta(y_1)=\gamma_1(a)=\text{d} & \text{because of} & 1 \equiv 1(mod\,3)\\
\text{for } i=2, & \delta(y_2)=\gamma_2(n)=\text{i} & \text{because of} & 2 \equiv 2(mod\,3)\\
\text{for } i=3, & \delta(y_3)=\gamma_3(k)=\text{l} & \text{because of} & 3 \equiv 0(mod\,3)\\
\text{for } i=4, & \delta(y_4)=\gamma_1(a)=\text{d} & \text{because of} & 4 \equiv 1(mod\,3)\\
\text{for } i=5, & \delta(y_5)=\gamma_2(r)=\text{ş} & \text{because of} & 5 \equiv 2(mod\,3)\\
\text{for } i=6, & \delta(y_6)=\gamma_3(a)=\text{c} & \text{because of} & 6 \equiv 0(mod\,3)
\end{array}$$

Therefore,

y_t	a	n	k	a	r	a
$\delta(y_t)$	d	i	l	d	ş	c

This example is demonstrated in Figure 3.

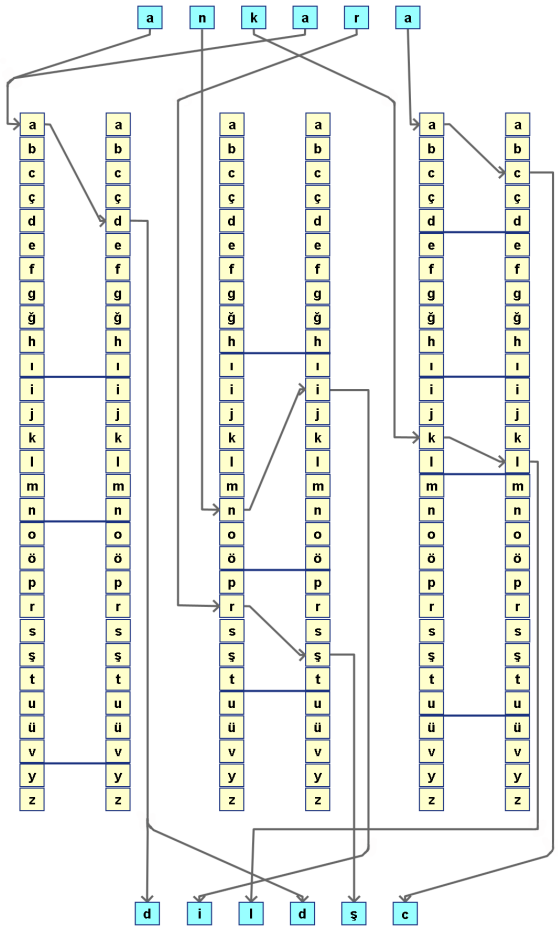


Figure 3: Encrypting the word of "ankara" by FP-cipher

3.3 FP-cipher Decryption Algorithm

In this subsection, we give an algorithm of the FP-cipher decryption method.

Assume that all of characters in a ciphertext are indexed as $s_1 s_2 ... s_q$. Here, we have to use the same values of P_i and R_i are obtained in the encryption. Then, an algorithm of the FP-cipher decryption is set up as follow.

Algorithm of FP-cipher Decryption

Step 1 : Find the values of γ_i^{-1} for $i \in I_k$,
Step 2 : Find the values $\delta^{-1}(s_t)$ for all $t \in I_q$.

Example 26. Let us consider Example 25 where "ankara" was encrypted as "dildşc". Now, the cipher text "dildşc" is decrypted. Here, we have to use same values of P_i and R_i in Example 25. Assume that this ciphertext is indexed as $s_1 s_2 s_3 s_4 s_5 s_6$ and decrypted by 3-FP-cipher decryption. Then,

Step 1 : For $i = 1, 2, 3$, the values $\gamma_i^{-1}(x)$ are obtained as follow,

x	a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö
$\gamma_1^{-1}(x)$	d	e	f	g	ğ	h	ı	a	b	c	ç	m	n	i	j	k	l	ş	t
$\gamma_2^{-1}(x)$	ç	d	e	f	g	ğ	h	a	b	c	l	m	n	o	ö	ı	i	j	k
$\gamma_3^{-1}(x)$	c	ç	d	a	b	g	ğ	h	ı	e	f	j	k	l	i	ö	p	r	s

$\gamma_1^{-1}(x)$	u	ü	v	o	ö	p	r	s	z	y
$\gamma_2^{-1}(x)$	s	ş	t	p	r	y	z	u	ü	v
$\gamma_3^{-1}(x)$	ş	t	u	m	n	o	v	y	z	ü
x	p	r	s	ş	t	u	ü	v	y	z

Step 3 : For all $t \in I_6$, the values $\delta^{-1}(s_t)$ are obtained as follow,

$$\begin{aligned}
&\text{for } i=1, \quad \delta^{-1}(s_1) = \gamma_{(1)}^{-1}(s_1) = \text{a} \quad \text{because of} \quad 1 \equiv 1 (mod\, 3)\\
&\text{for } i=2, \quad \delta^{-1}(s_2) = \gamma_{(2)}^{-1}(s_2) = \text{n} \quad \text{because of} \quad 2 \equiv 2 (mod\, 3)\\
&\text{for } i=3, \quad \delta^{-1}(s_3) = \gamma_{(3)}^{-1}(s_3) = \text{k} \quad \text{because of} \quad 3 \equiv 0 (mod\, 3)\\
&\text{for } i=4, \quad \delta^{-1}(s_4) = \gamma_{(1)}^{-1}(s_4) = \text{a} \quad \text{because of} \quad 4 \equiv 1 (mod\, 3)\\
&\text{for } i=5, \quad \delta^{-1}(s_5) = \gamma_{(2)}^{-1}(s_5) = \text{r} \quad \text{because of} \quad 5 \equiv 2 (mod\, 3)\\
&\text{for } i=6, \quad \delta^{-1}(s_6) = \gamma_{(3)}^{-1}(s_6) = \text{a} \quad \text{because of} \quad 6 \equiv 0 (mod\, 3)
\end{aligned}$$

Therefore,

s_t	d	i	l	d	ş	c
$\delta^{-1}(s_t)$	a	n	k	a	r	a

3.4 FP-cipher Program Codes

In this subsection, FP-cipher is programmed by using C# as follows:

```
private void btn_alfabe_olustur_Click(object sender, EventArgs e)
{
   //txtanahtar.Text = "";
   if (rdsifre.Checked)
```

```
{
    txtanahtar.Text = "";
    //anahtar oluşturma
    for (int i = 0; i < trczorluk.Value; i++)
    {
        System.Threading.Thread.Sleep(500);
        string anahtar = _anahtar(alf_metin().Length);
        txtanahtar.Text += anahtar.Substring(0,
                                    anahtar.Length - 1) + "*";
    }
}
//sanal matris oluşturma
DataTable matris = new DataTable();
for (int i = 0; i <alf_metin().Length; i++)
{
    matris.Columns.Add(alf_metin()[i]);
}
string[] key = txtanahtar.Text.Substring(0,
                        txtanahtar.Text.Length - 1).Split('*');
for (int i = 0; i < key.Length; i++)
{
    int alfabe_sayac = 1;
    string[] parca = key[i].Substring(0, key[i].Length).
                                            ToString().Split('-');
    string[][] U = new string[parca.Length][];//(Açık U)
    string[][] SU = new string[parca.Length][];//(Şifreli U)
    //alfabenin kümelere bölnmesi
    for (int j = 0; j < parca.Length; j++)
    {
        string[] parca_a = parca[j].ToString().Split(',');
        int P = int.Parse(parca_a[0]); //parça anahtarı
        U[j] = new string[alf_metin().Length+1];
        SU[j] = new string[alf_metin().Length+1];
        for (int x = 0; x < P; x++)
        {
            U[j][alfabe_sayac] = alf_metin()[alfabe_sayac-1];
            alfabe_sayac++;
        }
    }
    //alfabenin şifrelenmesi
    int m = 0;
    int indis = 1;
    for (int j = 0; j < U.Length; j++)
    {
        string[] parca_a = parca[j].ToString().Split(',');
        int P = int.Parse(parca_a[0]); //parça anahtarı
        int R = int.Parse(parca_a[1]); //öteleme anahtarı
```

```
            m += P;
            for (int x = 0; x < P; x++)
            {
                int k = 0;
                if ((indis+R)<=m) //öteleme fonksiyonu
                {
                    k = indis + R;
                }
                else if ((indis + R) > m)
                {
                    k = ((indis + R) % m)+(m-P);
                }
                SU[j][indis] = U[j][k];
                indis++;
            }
        }
        //matrise değerlerin eklenmsi
        matris.Rows.Add();
        int alsayac = 0;
        for (int j = 0; j < U.Length; j++)
        {
            string[] parca_a = parca[j].ToString().Split(',');
            int P = int.Parse(parca_a[0]); //parça anahtarı
            for (int x = 0; x < P; x++)
            {
                matris.Rows[i][alsayac] = SU[j][alsayac + 1];
                alsayac++;
            }
        }
        dataGridView1.DataSource = matris;
    }
}
```

4 Conclusions

In this work, we defined the FP-cipher that is a generalization of the Vigenere cipher. The Vigenere cipher is a type of polyalphabetic cipher in which different shift ciphers are used to encryption. In the FP-cipher, plaintext is encrypted by multiple encryption alphabets which are obtained by using the FC-cipher. Therefore, the key space of FP-cipher cipher has more possibility then the Vigenere cipher. We then constructed a mathematical modeling and make a computer program of the method.

References

[1] Y. Aydoğan, N. Çağman, I. Şimşek, Fragmented Caesar Cipher, Journal of New Theory 14 (2016) 46-57.

[2] Y. Aydoğan, Multi Fragmented Caesar Cipher Method and its Applications (in Turkish), MSc Thesis, Gaziosmanpasa University, Graduate School of Natural and Applied Science, 2014.

[3] J. Hoffstein, J. Pipher and J. H. Silverman, An Introduction to Mathematical Cryptograph, Springer-Newyork, 2008.

[4] C. Paar, J. Pelzl, Understanding Cryptograph, Springer-Verlag, 2010.

[5] A. Sinkov, Elementary Cryptanalysis - A Mathematical Approach, New Mathematical Library, No. 22, Mathematical Association of America, 1966.

http://www.newtheory.org **ISSN: 2149-1402**

Journal of New Theory

Year: **2016**, *Number*: **14**, *Pages*: **73**

EDITORIAL

We are happy to inform you that Number 14 of the Journal of New Theory (JNT) is completed with 6 articles.

JNT publishes original research articles, reports, reviews and commentaries that are based on a theory of mathematics. However, the topics are not limited to only mathematics, but also include statistics, computer science, physics, engineering, chemistry, biology, economics or social sciences that use a theory of mathematics.

JNT is a refereed, electronic, open access and international journal.

Papers in JNT are published free of charge.

We would like to express our deepest thanks to all of the members of the editorial board and reviewers of the papers in this issue who are U. Orhan, A. Filiz, A. Fenercioğlu, A. Sarı, A. Yıldırım, A. S. Sezer, B. Mehmetoğlu, B.H. Çadırcı, C. Kaya, Ç. Çekiç, D. Mohamad, E. Altuntaş, E. Turgut, F. Karaaslan, F. Smarandache, G. Erdal, H. Aktaş, H.M. Doğan, H. Günal, H. Kızılaslan, H. Önen, H. Şimşek, İ. Zorlutuna, İ. Deli, İ. Gökce, İ. Türkekul, İ. Parmaksız, J. Zhan, J. Ye, H. Kızılaslan, M. Akar, M. Akdağ, M.I. Ali, M. Ali, M. Çavuş, M. Demirci, N. Çağman, N. Sağlam, N. Yeşilayer, N. Kızılaslan, O. Muhtaroğlu, P.K. Maji, R. Yayar, S. Broumi, S. Karaman, S. Tarhan, S. Enginoğlu, S. Demiriz, S. Karataş, S. Öztürk, S. Eğri, Ş. Sözen, Y. Budak, E. S. Başcı, M. Arshad.

Pleases, write any original idea. If it is true, it gives an opportunity to use. If it is incomplete, it gives an opportunity to complete. If it is incorrect, it gives an opportunity to correct.

You can reach us from journal homepage at http://www.newtheory.org. To receive further information and to send your recommendations and remarks, or to submit articles for consideration, please e-mail us at jnt@newtheory.org

We hope you will enjoy this issue of JNT. We are looking forward to hearing your feedback and receiving your contributions.

Happy reading!

24 July 2016

Prof. Dr. Naim Çağman
Editor-in-Chief
Journal of New Theory
http://www.newtheory.org